527,820

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年1 月27 日 (27.01.2005)

PCT

(10) 国際公開番号
WO 2005/008502 A1

(51) 国際特許分類[7]: G06F 12/14, G06K 17/00

(21) 国際出願番号: PCT/JP2004/010432

(22) 国際出願日: 2004 年7 月15 日 (15.07.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-275672 2003 年7 月16 日 (16.07.2003) JP
特願2004-197453 2004 年7 月2 日 (02.07.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真1006番地 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 高木 佳彦 (TAKAGI, Yoshihiko). 菊地 隆文 (KIKUCHI, Takafumi).

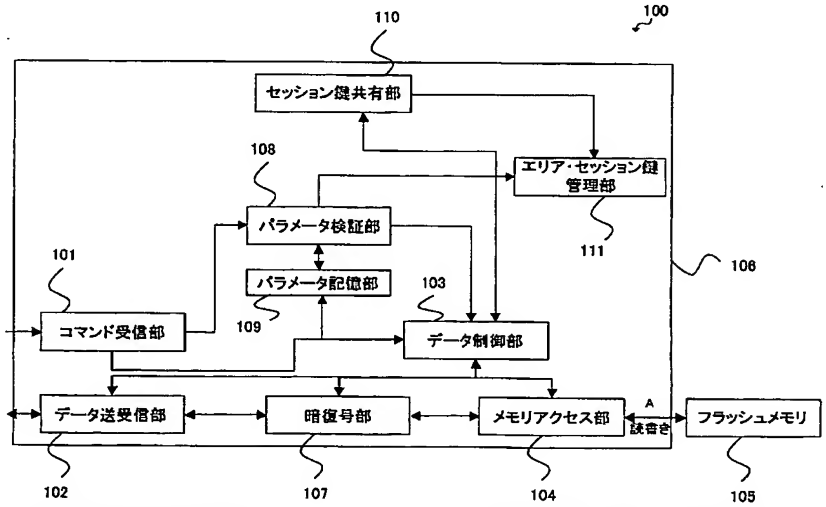
(74) 代理人: 鷲田 公一 (WASHIDA, Kimihito); 〒2060034 東京都多摩市鶴牧1丁目24-1 新都市センタービル5階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[続葉有]

(54) Title: ACCESS METHOD

(54) 発明の名称: アクセス方法



(57) Abstract: A command specifying an access region from a terminal is separated from a command performing access and the argument of the command performing access contains terminal verification data when transmitted. Thus, it is possible to verify that the terminal application which has issued the command specifying the access region, the terminal application which has issued the command performing access, and the terminal application holding the authentication key are the same.

(57) 要約: 端末からアクセス領域を指定するコマンドと、アクセスを行うコマンドを分離し、アクセスを行うコマンドの引数に端末の検証データを含めて送信することで、アクセス領域を指定するコマンドを発行した端末アプリケーションとアクセスを行うコマンドを発行した端末アプリケーションと、検証用鍵を保有する端末アプリケーションが同一であることが検証可能となる。

WO 2005/008502 A1

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明　細　書

アクセス方法

技術分野

本発明は、ＰＣや携帯電話などの端末に挿入して使用されるメモリカード、並びにメモリカードに対するアクセス方法に関する。

背景技術

従来、メモリカードは端末に挿入され、端末がデータを格納するためのものである。以下に、従来のメモリカードの一例をあげる（例えば、特願２００３－９１７０４号公報）。

カードは、端末から各種コマンドを受け付け、またコマンドに対するレスポンスを返すコマンド用端子（ＣＭＤライン）と、データの入力を受け付け、またデータの出力を行うデータ用端子（ＤＡＴライン）を持つ。

図１に示した従来のメモリカードの例では、端子４６０２がＣＭＤラインとなっており、端子４６０７、４６０８、４６０９がＤＡＴラインであり、それぞれＤＡＴ０、ＤＡＴ１、ＤＡＴ２となっている。また端子Ｃ２－０１はデータ入出力用とカード検出用（ＣＤ）を兼ねたＣＤ／ＤＡＴ３となっている。ＤＡＴ０～ＤＡＴ３については、ＤＡＴ０のみを使うモードと、ＤＡＴ０～３を同時に利用しＤＡＴ０のみを使う場合の４倍の転送速度を実現するモードが存在する。

次に、図２を用いて、従来カードのカード内モジュール構成について説明する。

カード内モジュールは、ＣＭＤライン４６０２に接続された、コマンド受信及びレスポンス送信を行う処理命令受信手段４７０１と、ＤＡＴライン４６０７、４６０８、４６０９、Ｃ２－０１に接続された、データ送受信を行うデー

タ送受信手段４７０２と、記憶領域４７０４と、受信したコマンドに応じて記憶領域４７０４へのデータの読み書きを行う記憶領域アクセス手段４７０３からなる。

次に、従来のメモリカードにおける、データ読み出し時の処理動作について説明する。ここではデータの出力はＤＡＴ０端子４６０７のみを利用するモードに設定されているものとするが、ＤＡＴ１端子４６０８、ＤＡＴ２端子４６０９、ＤＡＴ３端子４６１０を併用するモードであってもよい。

まず、端末はカードのＣＭＤライン４６０２にデータ読み出しコマンドを送信する。この読み出しコマンドは図７で示されるフォーマットとなっており、６ビットのコマンドコード４０１と３２ビットのコマンド引数４０２から構成される。データ読み出しコマンドにおけるコマンド引数は、読み出し開始アドレスを格納する。

端末からコマンドを受信した処理命令受信手段４７０１は、コマンドコード４０１を参照して、データ読み出しコマンドであることを認識する。

次に、処理命令受信手段４７０１は、コマンド引数４０２を参照して、指定されたアドレスが正しいものであるか、つまりカードが対応している範囲に指定されたアドレスが収まっているかを調べ、アドレスが正しくなければレスポンスとしてエラーである旨のレスポンスコードを返す。アドレスが正しければ正常である旨のレスポンスコードを返す。

処理命令受信手段４７０１は、レスポンスを端末に返送した後、記憶領域アクセス手段４７０３に対し、指定されたアドレスとともに、読み出し要求を行う。

記憶領域アクセス手段４７０３は、記憶領域４７０４の指定アドレスからデータを読み出し、データ送受信手段４７０２に送信する。

データ送受信手段４７０２は、ＤＡＴ０ライン４６０７を通じて、端末に読み出しデータの出力を行う。

このようなメモリカードでは、端末からアドレスを指定して自由にカードの

読み書きが可能である。

上記のようなメモリカードにおいて、フラッシュメモリの特定領域をセキュリティ保護領域としてアクセス制限をかけ、アクセスが許可された特定の端末からのみアクセス可能としたい場合に、上記文献で示されたカードでは、ＩＣカードコマンドを用いて柔軟な認証を行うことが可能である。しかし、ＩＣカードの標準的なコマンドフォーマットであるＡＰＤＵ（Application protocol data unit）では、２５６バイトのデータ送受信しか行えないことと、半二重プロトコルのために、ホストからのコマンド送信の度にレスポンス受信が必要であるという理由から、高速なデータ転送が困難である。そこで、ＩＣカードコマンドを用いて、セキュリティポリシーに柔軟にあわせた方式にて認証処理を行った後でメモリカードコマンドを用いてデータ転送を行う方式が考えられるが、ＩＣカードコマンドの発行者とメモリカードコマンドを発行したホスト上のアプリケーションが同一であることを確認することが困難である。

そこで、ＩＣカードコマンドを用いた認証処理の過程で生成した情報を、ＩＣカードコマンドとメモリカードコマンドの発行者の同一性を検証するための検証データとしてメモリカードコマンドに含める場合、コマンド引数にアクセス領域指定情報（アクセスするアドレスなど）と認証用の検証データを含めることになるが、データ読み出しコマンドのコマンド引数４０２のサイズは上述の通り、３２ビットの固定であるので、セキュリティを向上させるため認証用の検証データのサイズを大きくすると、アクセス領域指定情報の長さが短くなりアクセス可能な領域が制限されてしまう。一方、検証データのサイズを小さくすれば、セキュリティ強度が下がってしまう。

この課題を解決するために、従来のデータ読み出しコマンドのフォーマットを変更すると、従来のメモリカードにアクセスができなくなってしまうおそれがある。

また、従来のデータ読み出しコマンドと、セキュリティ保護領域を備えたメモリカードへのデータ読み出しコマンドとを別個のものとして併存させると

すると、端末側でメモリカードの種類によってコマンドを切り換える必要が発生し、メモリカードへのアクセスが複雑となり、端末にとっては利用しづらいものとなる。そのため、検証データを送信するためのコマンドとデータの読み出しまたは書き込みを行うためのメモリカードコマンドをそれぞれ定義し、2つのコマンドを組み合わせてセキュリティ保護領域へのアクセスを行う必要があるが、2つのコマンドの間でコマンド発行者の同一性を確認することができない。

発明の開示

本発明は、これらの問題点を解決するものであり、メモリカード内でアクセス制限がされていない領域にアクセスする場合は、上述のデータ読み出しコマンドに代表されるメモリカードコマンドを用い、アクセス制限がされているセキュリティ保護領域に関しては、まずアクセス領域を指定するメモリカードコマンドによってアクセス領域指定情報をメモリカードに送付した後に、ホストとメモリカード間でＩＣカードコマンドを用いた柔軟な認証処理を用いて共有した、または、予め共有している鍵情報と、上記アクセス領域指定情報を用いて生成した認証用の検証データを含ませた、セキュリティ保護領域の読み出しまたは書き込み用メモリカードコマンドをメモリカードに送付して、セキュリティ保護領域へのデータの書き込み、セキュリティ保護領域からのデータを読み出しする、という2段階のコマンド構成にすることで、メモリカードコマンドのフォーマットの変更を必要とせず、また少ないコマンド引数でもセキュリティを低下させることなく、セキュリティ保護領域へのアクセスを可能にするアクセス方法を提供することを目的とする。

本発明の一形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、前記メモリ

デバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有する。

本発明の他の形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、前記可能領域情報を参照し、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有する。

本発明のさらに他の形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、検証用鍵を共有化するステップと、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有する。

本発明のさらに他の形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、前記メモリデバイスとで、前記アクセス可能領域に対応した検証用鍵を共有化するステップと、前記可能領域情報を参照し、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス

領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有する。

本発明のさらに他の形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、第一の処理系コマンドを用いて、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、前記可能領域情報を参照し、第二の処理系コマンドを用いて、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有する。

本発明のさらに他の形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、第一の処理系コマンドを用いて、検証用鍵を共有化するステップと、第二の処理系コマンドを用いて、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有す

る。

本発明のさらに他の形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記メモリデバイスは、前記機器からのアクセスが制約された耐タンパ性の第１領域と、前記機器からのアクセスが制約された非耐タンパ性の第２領域と、前記機器からアクセスすることが可能な第３領域と、を有し、少なくとも前記第１領域への処理命令である第一の処理系コマンドと、少なくとも前記第３領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、前記機器は、前記メモリデバイスとで、第一の処理系コマンドを用いて、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、前記可能領域情報を参照し、第二の処理系コマンドを用いて、前記第２領域へのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、前記メモリデバイスは、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有する。

本発明のさらに他の形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記メモリデバイスは、前記機器からのアクセスが制約された耐タンパ性の第１領域と、前記機器からのアクセスが制約された非耐タンパ性の第２領域と、前記機器からアクセスすることが可能な第３領域と、を有し、少なくとも前記第１領域への処理命令である第一の処理系コマンドと、少なくとも前記第３領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、前記機器は、前記メモリデバイスとで、第一の処理系コマンドを用いて、検証用鍵を共有化するステップと、第二の処理系コマンドを用いて、前記第２領域へのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命

令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスは、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有する。

本発明のさらに他の形態によれば、メモリデバイスは、機器から読み書きされるメモリデバイスであって、アクセスする領域を指定する指定情報を受信するとともに、前記指定情報に基づく検証情報と読み出し又は書き込み命令を併せて受信する処理命令受信手段と、前記指定情報を、前記検証情報を用いて検証処理を行う指定情報検証手段と、データを格納する記憶領域と、前記検証処理が成功した場合に、前記処理命令に応じて、前記記憶領域の前記指定領域に対する読み出し又は書き込みを行う記憶領域アクセス手段と、前記記憶領域アクセス手段が読み出したデータを前記機器に送信するデータ送信手段と、前記機器から書き込みデータを受信するデータ受信手段と、を備える。

本発明のさらに他の形態によれば、情報機器は、メモリデバイスを読み書きする情報機器であって、読み出し又は書き込みする領域を決定し、前記領域を指定する指定情報を決定する指定情報決定手段と、前記指定情報から前記検証情報の生成処理を行う検証情報生成手段と、前記指定情報の送信と、前記検証情報と読み出し又は書き込みの処理命令とを併せて送信する処理命令送信手段と、前記処理命令が書き込みの場合は、前記メモリデバイスにデータを送信するデータ送信手段と、前記処理命令が読み出しの場合は、前記メモリデバイスからデータを受信するデータ受信手段と、前記メモリデバイスに送信するデータを記憶し、または、前記メモリデバイスから受信したデータを記憶するデータ記憶手段と、を備える。

本発明のさらに他の形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処

理命令と、前記指定情報に関する検証情報を検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと検証用鍵とを用いて検証するステップと、前記検証に成功した場合、前記処理命令を実行するステップと、を有する。

本発明のさらに他の形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記機器は、第一の処理系コマンドを用いて前記メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、第一の処理系コマンドを用いて前記アクセス可能領域に対応した検証用鍵を共有化するステップと、第二の処理系コマンドを用いて、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスは、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合は、前記処理命令を実行するステップと、を有する。

本発明のさらに他の形態によれば、アクセス方法は、機器からメモリデバイスに対するアクセス方法であって、前記メモリデバイスは、前記機器からのアクセスが制約された耐タンパ性の第１領域と、前記機器からのアクセスが制約された非耐タンパ性かつ大容量の第２領域と、前記機器からアクセスすることが可能なかつ大容量の第３領域と、を有し、少なくとも前記第１領域への処理命令である第一の処理系コマンドと、少なくとも前記第３領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、前記機器は、前記メモリデバイスとで、第一の処理系コマンドを用いて、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、第一の処理系コマンドを用いて、前記アクセス可能領域に対応した検証用鍵を共有化するス

テップと、第ニの処理系コマンドを用いて、前記第２領域へのアクセス領域を指定する指定情報を送信するステップと、第ニの処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスは、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有する。

図面の簡単な説明

図１は、従来のメモリカードの端子構成を示す図、

図２は、従来のカード内モジュール構成を示す図、

図３は、本発明の実施の形態１に係るメモリカードの内部モジュール構成を示す図、

図４は、本発明の実施の形態１に係るカードの端子構成を示す図、

図５は、本発明の実施の形態１に係る端末の内部構成を示す図、

図６は、本発明の実施の形態１に係るカードと端末の間で行われる処理の概要を示す図、

図７は、本発明の実施の形態１に係るＡＰＤＵの送受信方法のシーケンスを示す図、

図８は、本発明の実施の形態１に係るレスポンスＡＰＤＵの送信処理のシーケンスを示す図、

図９は、本発明の実施の形態１に係るメモリカードのコマンドフォーマットを示す図、

図１０は、本発明の実施の形態１に係るフラッシュメモリの内部構成を示す図、

図１１は、本発明の実施の形態１に係るセキュリティ保護領域の内部構成を

示す図、

図１２は、本発明の実施の形態１に係るセキュリティ保護領域内の各アプリケーション用領域の内部構成を示す図、

図１３は、本発明の実施の形態１に係るセッション鍵共有及びアクセス可能領域共有手順を示す図、

図１４は、本発明の実施の形態１に係る図１３のステップ９０３における処理の詳細を説明するためのフローチャート、

図１５は、本発明の実施の形態１に係る図１３のステップ９０５における処理の詳細を説明するためのフローチャート、

図１６は、本発明の実施の形態１に係る図１１のステップ９０７における処理の詳細を説明するためのフローチャート、

図１７は、本発明の実施の形態１に係る端末からセキュリティ保護領域を読み出すためのコマンドシーケンスを示す図、

図１８は、本発明の実施の形態１に係るＡＰＤＵ送信コマンドの引数フォーマットを示す図、

図１９は、本発明の実施の形態１に係るＡＰＤＵ受信コマンドの引数フォーマットを示す図、

図２０は、本発明の実施の形態１に係るＡＰＤＵ送信コマンドの入力データ及びＡＰＤＵ受信コマンドの出力データのフォーマットを示す図、

図２１は、本発明の実施の形態１に係るアクセス領域指定コマンドの入力データフォーマットを示す図、

図２２は、本発明の実施の形態１に係るアクセス領域指定情報を示す図、

図２３は、本発明の実施の形態１に係る端末の正当性検証を行うための検証データの端末による生成方法を示す図、

図２４は、本発明の実施の形態１に係る端末の正当性検証を行うための検証データのカードによる生成方法を示す図、

図２５は、本発明の実施の形態１に係る端末からセキュリティ保護領域に書

き込むためのコマンドシーケンスを示す図、

図２６は、本発明の実施の形態２に係るメモリカードの内部モジュール構成を示す図、

図２７は、本発明の実施の形態２に係る端末の内部構成を示す図、

図２８は、本発明の実施の形態２に係る端末からカードのセキュリティ保護領域に対してアクセスを行う際の処理を示すフローチャート、

図２９は、本発明の実施の形態２に係る領域指定命令のデータ部の一例を示す図、

図３０は、本発明の実施の形態２に係る図２９のアクセス領域指定情報のフォーマットを示す図、

図３１は、本発明の実施の形態２に係る比較情報の生成方法の一例を示す図、

図３２は、本発明の実施の形態２に係る内部に検証用鍵共有手段を備える場合のカード構成を示す図、

図３３は、本発明の実施の形態２に係る内部に検証用鍵共有手段を備える場合の端末構成を示す図、

図３４は、本発明の実施の形態２に係る検証用鍵の共有方法のシーケンスを示す図、

図３５は、本発明の実施の形態２に係る検証用鍵生成方法を説明するための図、

図３６は、本発明の実施の形態２に係るＳＨＡ－１演算を用いた比較情報生成方法を示す図、

図３７は、本発明の実施の形態２に係る検証情報生成方法を示す図、

図３８は、本発明の実施の形態２に係るアクセス命令のフォーマットを示す図、

図３９は、本発明の実施の形態２に係る数情報を利用した検証データ生成処理を示すフローチャート、

図４０は、本発明の実施の形態２に係る乱数を利用した比較情報生成方法を

示す図、

図４１は、本発明の実施の形態２に係る乱数を利用した検証情報生成方法を示す図、

図４２は、本発明の実施の形態３に係るメモリカードの内部モジュール構成を示す図、

図４３は、本発明の実施の形態３に係る端末の内部構成を示す図、

図４４は、本発明の実施の形態３に係る端末からカード内のセキュリティ保護領域へのアクセス処理の一部を示すフローチャート、

図４５は、本発明の実施の形態３に係る図４４に続くアクセス処理の一部を示すフローチャート、

図４６は、本発明の実施の形態３に係るアクセス有効テーブルの一例を示す図、

図４７は、本発明の実施の形態１に係るアクセス有効テーブルの一例を示す図である。

発明を実施するための最良の形態

以下、本発明の実施の形態について、添付図面を参照して詳細に説明する。なお、本発明は、この実施の形態に何ら限定されるものではなく、その要旨を逸脱しない範囲において、種々の形態で実施することができる。

（実施の形態１）

本発明におけるカード内モジュール構成について図３を用いて説明する。なお、カード１００の端子配置は、図４に示すが、その端子構成は、図１に示したものと各端子に付した符号は異なるが、その構成は同様であるため、説明は省略する。

カード内モジュールは、コントローラ１０６とフラッシュメモリ１０５からなる。コントローラ１０６は、ＣＭＤラインに接続された、コマンド受信及びレスポンス送信を行うコマンド受信部１０１と、ＤＡＴラインに接続されたデ

ータ送受信部１０２と、データ送受信部１０２が送受信したデータに対してセッション鍵で暗復号処理を施し、またフラッシュメモリ格納用鍵で暗復号してメモリアクセス部１０４とのデータ受け渡しを行う暗復号部１０７と、フラッシュメモリ１０５へのデータの読み書きを行うメモリアクセス部１０４と、受信したコマンドに応じて、メモリアクセス部１０４、セッション鍵共有部１１０、及びパラメータ検証部１０８、暗復号部１０７に対して処理要求を行うデータ制御部１０３と、端末２００から受信したセキュリティ保護領域にアクセスするためのパラメータを記憶しておくパラメータ記憶部１０９と、パラメータが正しいことを検証するパラメータ検証部１０８と、端末２００との間で認証用及び暗復号用のセッション鍵を交換するセッション鍵共有部１１０と、セッション鍵と、セッション鍵と対応付けられたセキュリティ保護領域を記憶しておくエリア・セッション鍵管理部１１１からなる。

次に、本実施の形態１における端末２００の構成について図５を用いて説明する。

端末２００は、カード１００にメモリカードコマンドを送信するコマンド送信部２０４と、カード１００のＤＡＴラインにデータを送信するデータ送受信手段２０７と、データ送受信手段２０７が送信するデータを暗号化し、また受信するデータを復号化する暗復号手段２０６と、カード１００との間でセッション鍵の共有処理を行うセッション鍵共有手段２０２と、セキュリティ保護領域アクセスコマンドによってアクセスする領域を決定し、領域指定情報を生成する、指定情報決定手段２０１と、領域指定情報とセッション鍵から検証データを生成する検証データ生成部２０３と、送信するデータ、または受信したデータを記憶するデータ記憶手段２０５とを備える。

次に、図３のカード１００と図５の端末２００の間で行われる処理の概要について図６を用いて説明する。

図６において、まず、端末２００とカード１００の間では、カード１００ＩＣカードコマンドを用いた処理として、端末２００とカード１００相互間を認

証するための認証処理及びセッション鍵を共有するための鍵共有処理と、端末２００からカード１００内メモリへのアクセス可能領域の領域番号（図中の領域Ｎｏ．ｘ）を割り当てる領域番号割り当て処理とが実行される（ステップＳ４０１）。

認証処理を行い、相互に正当性が確認された後、鍵共有処理及び領域番号割り当て処理が行われ、その結果として、端末２００内とカード１００内には、領域Ｎｏ．ｘにて示されるセキュリティ保護領域へのアクセスを可能にする検証用及び暗号用のセッション鍵が領域番号（領域Ｎｏ．ｘ）と対応付けて保持される。

次に、端末２００とカード１００の間では、メモリカードコマンドを用いた処理として、端末２００からカード１００へのアクセス領域指定コマンド送信処理（ステップＳ４０２）及びデータ転送コマンド送信処理（ステップＳ４０３）と、カード１００から端末２００への暗号化データ送信処理（ステップＳ４０４）とが実行される。

アクセス領域指定コマンド送信処理では、アクセスしたいセキュリティ保護領域内の領域を指定するため、領域Ｎｏ．ｘ、ブロックアドレス及びブロック長を設定したデータを含むアクセス領域指定コマンドが端末２００からカード１００へ送信される。カード１００では、受信したアクセス領域指定コマンドから抽出した領域Ｎｏ．ｘに基づいてセキュリティ保護領域へのアクセス可否検証処理が実行される。

また、データ転送コマンド送信処理では、端末２００において領域Ｎｏ．ｘ、ブロックアドレス及びブロック長と、ステップＳ４０１にてカード１００との間で共有した検証用鍵を用いて検証データが作成され、この検証データを含むデータ転送（Ｒｅａｄ）コマンドがカード１００に送信される。カード１００では、受信したデータ転送（Ｒｅａｄ）コマンドから端末２００との間で共有した検証用鍵の公開鍵を用いて領域Ｎｏ．ｘ、ブロックアドレス及びブロック長を元に検証データを作成していることを確認することで、ステップＳ４０２

にて指定されたセキュリティ保護領域へのアクセス可否が検証される。

また、暗号化データ送信処理では、カード１００において上記検証処理においてアクセス可となったカードアプリケーションに対応する領域Ｎｏ．ｘに格納されたデータが、端末２００との間で共有した暗号用鍵を用いて暗号化され、この暗号化データが端末２００に送信される。

以下の説明では、上記処理概要に処理手順について詳細に説明する。

端末２００とセッション鍵共有部１１０との間で送受信されるコマンド形態は、一般的なＩＣカードで用いられるＡＰＤＵフォーマットに従った形とする。つまり、セッション鍵共有部１１０はＩＣカードアプリケーションの形態をとる。

ここでは、ＡＰＤＵの送受信方法について、図７のシーケンス図を用いて説明する。

まず、端末２００からカード１００に対するコマンドＡＰＤＵの送信処理について説明する。ここで、コマンドＡＰＤＵとは、メモリカード側で実行させたいコマンドをＡＰＤＵフォーマット形式で端末２００からメモリカード送付するものをいい、具体的にはＩＣカード用コマンドを使用する。

まず、端末２００はセッション鍵共有部１１０に対して送信するコマンドＡＰＤＵを作成する。次に、端末２００は図２のカード１００のＣＭＤライン２２に対して、ＡＰＤＵ送信コマンドを送信する（ステップＳ５０１）。

このＡＰＤＵ送信コマンドは、従来のデータ読み出しコマンドと同様、図７で示されるフォーマットとなっており、６ビットのコマンドコード４０１と３２ビットのコマンド引数４０２から構成される。

ＡＰＤＵ送信コマンドにおけるコマンド引数４０２は、図１８で示すように、ＤＡＴ０ライン２７に入力するデータがコマンドＡＰＤＵであることを示すフラグ１４０１と送信データ数を示す１４０３とからなる。フラグ１４０１及び送信データ数１４０３を合わせて３２ビットに満たない場合は未使用フィールド１４０２が存在する。

図４のＤＡＴ０ライン２７に入力するデータは５１２バイト単位となっており、送信データ数１４０３は、この５１２バイト単位の入力を何回行うかを示す。

次に、カード１００のコマンド受信部１０１は、端末２００から送信されたコマンドを受信し（ステップＳ５０２）、それがＡＰＤＵ送信コマンドであることを認識し、ＣＭＤライン２２を介して端末２００にレスポンスを返すとともに（ステップＳ５０３）、データ制御部１０３に対して、ＡＰＤＵ送信コマンドを受信したことを通知する（ステップＳ５０４）。

次に、端末２００はカード１００のＣＭＤライン２２からＡＰＤＵ送信コマンドに対するレスポンスを受信し（ステップＳ５０３）、ＤＡＴ０ライン２７に図２０で示すフォーマットでコマンドＡＰＤＵ１６０２を入力する（ステップＳ５０５）。

図２０において、１６０１で示される長さは後に続くＡＰＤＵ１６０２の長さを示している。長さフィールド１６０１とＡＰＤＵ１６０２の合計長にあわせてコマンド引数の送信データ数１４０３が設定されている。また、前記合計長は必ずしも５１２バイトの倍数になるわけではないので、５１２バイトの倍数になるようにパディング１６０３を付加する。

次に、カード１００内部のデータ送受信部１０２は、端末２００からＤＡＴ０ライン２７に入力されたコマンドＡＰＤＵを受信するとともに（ステップＳ５０５）、データ制御部１０３にコマンドＡＰＤＵを受信したことを通知する（ステップＳ５０６）。次に、データ制御部１０３は、データ送受信部１０２からコマンドＡＰＤＵを読み出し（ステップＳ５０７）、セッション鍵共有部１１０（ＩＣカードアプリケーション）にコマンドＡＰＤＵを渡す（ステップＳ５０８）

次に、セッション鍵共有部１１０は、コマンドＡＰＤＵに記述されたとおりの処理を行い（ステップＳ５０９）、処理の結果生じたデータとステータス情報をレスポンスＡＰＤＵとしてデータ制御部１０３に渡す（ステップＳ５１

０）。このステータス情報とは、ＩＳＯ７８１６で定義されたステータスワードであり、正常終了したか、異常終了したかを示す２バイトの値である。

次に、カード１００から端末２００に対するレスポンスＡＰＤＵの送信処理について、図８のシーケンス図を用いて説明する。ここでレスポンスＡＰＤＵとは、カード１００が実行したコマンドＡＰＤＵの処理結果をカード１００から端末２００へ送信するものをいう。

ここでは、前記のコマンドＡＰＤＵの送信方法で示したとおり、セッション鍵共有部１１０が出力したレスポンスＡＰＤＵがデータ制御部１０３で保持されている状態であるものとする。

まず、端末２００は、カード１００のＣＭＤライン２２に対して、ＡＰＤＵ受信コマンドを送信する（ステップＳ６０１）。このＡＰＤＵ受信コマンドは、ＡＰＤＵ送信コマンドと同様、図９で示される従来のデータ読み出しコマンドと同様のフォーマットとなっており、６ビットのコマンドコード４０１と３２ビットのコマンド引数４０２から構成される。

ＡＰＤＵ受信コマンドにおけるコマンド引数４０２は、図１９で示すように、未使用フィールド１５０１と送信データ数１５０２とからなる。送信データ数１５０２が３２ビットに満たない場合は未使用フィールド１５０１が存在する。

図４のＤＡＴ０端子２７から出力されるデータは、ＡＰＤＵ送信コマンドにおける入力データと同様に５１２バイト単位となっており、送信データ数１５０２は５１２バイト単位で何回出力を行うかを示す。

次に、カード１００のコマンド受信部１０１は、端末２００から送信されたコマンドを受信し（ステップＳ６０２）、それがＡＰＤＵ受信コマンドであることを認識し、ＣＭＤライン２２を介して端末２００にレスポンスを返すとともに（ステップＳ６０３）、データ制御部１０３に対して、ＡＰＤＵ受信コマンドを受信したことを通知する（ステップＳ６０４）。

次に、データ制御部１０３は、データ送受信部１０２に対して、セッション

鍵共有部１１０から受け取ったレスポンスＡＰＤＵを渡す（ステップＳ６０５）。

次に、端末２００は、カード１００のＣＭＤライン２２からＡＰＤＵ受信コマンドに対するレスポンスを受信し（ステップS.６０３）、ＤＡＴ０ライン２７を介してデータ送受信部１０２からレスポンスＡＰＤＵを読み出す（ステップＳ６０６）。読み出されるレスポンスＡＰＤＵは、図２０で示すフォーマットで出力される。各フィールドの詳細については、ＡＰＤＵ送信コマンドにおける入力時と同様であるため、説明を省略する。

カード１００に搭載されるフラッシュメモリ１０５は、図１０に示すように、少なくとも端末２００から従来の読み出し用コマンド及び書き込み用コマンドに代表されるメモリカードコマンドでアクセスすることが可能な通常領域（非耐タンパ性のメモリ領域）６２と、前記の従来のコマンドではアクセスすることができないセキュリティ保護領域（耐タンパ性のメモリ領域）６１を持つ。また、カード１００は、図１０に示すように、ＩＣカードコマンドでアクセスすることが可能な耐タンパ領域（ＴＲＭ：tamper resistant module ）８０を持つ。

セキュリティ保護領域６１は、通常、カードアプリケーションからのみアクセス可能な状態であって、端末２００からの従来の読み出し用コマンド及び書き込み用コマンドに対しては、コマンド受信部１０１によってアクセスは排除される。

本発明におけるメモリカードは内部に複数のカードアプリケーションを搭載することが可能となっており、図１１に示すように、セキュリティ保護領域６１は各アプリケーションに対して個別の領域（ＡＰ１用領域７１～ＡＰ３用領域７３）を割り当てることが可能である。

セキュリティ保護領域６１は、データ制御部１０３が管理する格納用暗号鍵（Ｋｓ）で暗号化されている。この暗号鍵は、セキュリティ保護領域６１全体で１つのＫｓであってもよいし、各アプリケーション用のＡＰ１用領域７１～

ＡＰ３用領域７３に個別に格納用暗号鍵Ｋｓ＿１～Ｋｓ＿３を用意してもよい。本実施の形態では各アプリケーションＡＰ１～３に格納用暗号鍵Ｋｓ＿１～Ｋｓ＿３を用意する。

次に、セキュリティ保護領域６１内の各アプリケーション用のＡＰ１用領域７１～ＡＰ３用領域７３の内部構成について、図１２を用いて説明する。

ここでは、例としてカードアプリケーションＡＰ１用領域７１をあげている。ＡＰ１用領域７１の内部はディレクトリＤＩＲ１，ＤＩＲ２とファイルＦＩＬＥ１～ＦＩＬＥ３を用いた階層構造を用いたデータ管理となっている。

カードアプリケーションＡＰ１は、ＡＰ１用領域７１内でディレクトリ移動を行い、目的のファイルが存在するディレクトリＤＩＲ１，ＤＩＲ２上でファイルＦＩＬＥ１～ＦＩＬＥ３に対する読み書きを行う。

例えば、カードアプリケーションＡＰ１がファイルＦＩＬＥ３にアクセスする場合は、ディレクトリＤＩＲ１に移動し、次にディレクトリＤＩＲ２に移動した後、ファイルＦＩＬＥ３の読み書きを行う。また、各ディレクトリＤＩＲ１，ＤＩＲ２において、その下位のディレクトリまたはファイルの作成及び削除が可能である。

次に、カード１００内のセッション鍵共有部１１０と、端末２００との間で行われるセッション鍵共有手順について図１３～図１６を用いて説明する。

カードアプリケーションと端末２００はそれぞれ公開鍵暗号で用いられる公開鍵と秘密鍵の対を保持し、お互いに相手の公開鍵を保持している。

セッション鍵共有手順におけるコマンド形態は前記で示したＡＰＤＵを用いる。以降の説明においてはコマンド形態に関する記述を行わず、単にコマンドＡＰＤＵ、レスポンスＡＰＤＵと表記する。

まず、端末２００は、ＳＥＬＥＣＴコマンドＡＰＤＵを送信することで、カードアプリケーションＡＰ１の選択を行う（ステップ９０１）。ＳＥＬＥＣＴコマンドＡＰＤＵとは、以降のＩＣカードコマンド（コマンドＡＰＤＵ）をカード１００内部のどのアプリケーションに送信するかを指定するコマンドＡ

ＰＤＵであり、他のコマンドＡＰＤＵと同様にＡＰＤＵ送信コマンドを用いて送信する。

カード１００は、端末２００から指定されたカードアプリケーションＡＰ１の選択が正常に完了すれば正常完了のレスポンスＡＰＤＵ、完了しなければ異常終了のレスポンスＡＰＤＵを返す（ステップ９０２）。

次に、端末２００は、処理９０３を実行する。この処理９０３について簡単に説明すると、選択したカードアプリケーションＡＰ１にアクセスすることを可能にするＤＡＴＡ２を生成するための処理である。この処理９０３の詳細については、図１４のフローチャートを参照して説明する。

端末２００は、乱数Ｒｈの生成を行い（ステップＳ９０３１）、乱数Ｒｈと、端末２００がアクセスしたい図１２で示したファイルＦＩＬＥ３のファイル名を結合し、カードアプリケーションＡＰ１が保持する秘密鍵ＰｒｉＳに対応した公開鍵ＰｕｂＳで暗号化してＤＡＴＡ１を生成し（ステップＳ９０３２）、さらに端末２００が保持する秘密鍵ＰｒｉＨに対応した公開鍵ＰｕｂＨを示す識別子Ｉｎｆｏ＿ＰｕｂＨとＤＡＴＡ１を結合してＤＡＴＡ２を生成する（ステップＳ９０３３）。

図１３に戻り、次に、端末２００は、カードアプリケーションとのセッション鍵の共有及び、端末２００がアクセス可能な領域情報の共有を行うために、ステップＳ９０３３で生成したＤＡＴＡ２を含んだＲＥＱ＿ＡＲＥＡ＿ＩＮＦＯコマンドをカードアプリケーションに送信する（ステップ９０４）。

ＲＥＱ＿ＡＲＥＡ＿ＩＮＦＯコマンドを受信したカードアプリケーションＡＰ１は、処理９０５を実行する。この処理９０５の詳細については、図１５のフローチャートを参照して説明する。

カードアプリケーションＡＰ１は、ＤＡＴＡ２よりＤＡＴＡ１を抽出し、カードアプリケーションＡＰ１が保持する秘密鍵ＰｒｉＳで復号化し、乱数Ｒｈとファイル名ＦＩＬＥ３を得る（ステップＳ９０５１）。

次に、ＤＡＴＡ２より公開鍵を識別して識別子Ｉｎｆｏ＿ＰｕｂＨを抽出し、

Ｉｎｆｏ＿ＰｕｂＨが示す公開鍵ＰｕｂＨに対応付けられた端末２００によるアクセスが認められているかを、ファイルＦＩＬＥ３のアクセス権限設定を参照して確認する。権限がなければ、その旨のエラーをレスポンスＡＰＤＵとして端末２００に返す。アクセスする権限があれば、ＦＩＬＥ３のファイルサイズＳＩＺＥ３を取得する（ステップＳ９０５２）。

次に、乱数Ｒｓを生成し（ステップＳ９０５３）、ファイルＦＩＬＥ３に対する端末２００からのセキュリティ保護領域アクセスコマンドによるアクセスが可能となるように、図４７で示すアクセス有効テーブル４５００への登録を行い、端末２００がセキュリティ保護領域アクセスコマンドを用いてアクセスするときに使用するためのエリア番号Ｘをファイル ＦＩＬＥ３に割り当て、ファイルサイズＳＩＺＥ３とともにエリア・セッション鍵管理部１１１に記憶する（ステップＳ９０５４）。このエリア番号とは、端末２００がセキュリティ保護領域アクセスコマンドによるアクセスを行うときに、アクセス領域指定コマンドによって送信するアクセス領域指定情報に含める情報をいう。

次に、乱数Ｒｓ、エリア番号Ｘ、ファイルサイズＳＩＺＥ３を結合し、ＤＡＴＡ３を生成し（ステップＳ９０５５）、ＤＡＴＡ３を端末２００の公開鍵ＰｕｂＨで暗号化してＤＡＴＡ４を生成する（ステップＳ９０５６）。

次に、乱数Ｒｓと乱数Ｒｈに排他的論理和を施し、乱数Ｒを生成し（ステップＳ９０５７）、乱数Ｒから暗号用セッション鍵Ｋｄ、検証用セッション鍵Ｋｍを生成する（ステップＳ９０５８）。

次に、セッション鍵Ｋｄ及びＫｍをエリア番号Ｘと関連付け、エリア・セッション鍵管理部１１１に記憶する（ステップＳ９０５９）。

図１３に戻り、カード１００はここまでの処理を終えると端末２００にＤＡＴＡ４を含んだレスポンスＡＰＤＵを端末２００に送信する（ステップ９０６）。

レスポンスＡＰＤＵを受信した端末２００は、レスポンスＡＰＤＵからＤＡＴＡ４を抽出し、処理９０７を実行する。この処理９０７の詳細については、

図１６のフローチャートを参照して説明する。

端末２００は、端末２００の秘密鍵ＰｒｉＨを用いてＤＡＴＡ４を復号しＤＡＴＡ３を取得する（ステップＳ９０７１）。次に、端末２００は、ＤＡＴＡ３より乱数Ｒｓを取得し、乱数Ｒｓと乱数Ｒｈに排他的論理和を施し、乱数Ｒを生成し（ステップＳ９０７２）、乱数Ｒから暗号用セッション鍵Ｋｄ、検証用セッション鍵Ｋｍを生成する（ステップＳ９０７３）。

以上のステップ９０１から９０７を踏むことで、端末２００とカード１００間の相互認証を行い、かつ端末２００が指定したファイルに対するアクセス権限があれば端末２００からのアクセスが可能な状態となり、またアクセスする際に必要なエリア番号、エリア番号に割り当てられたファイルのサイズＳＩＺＥ３、および検証用セッション鍵Ｋｍ、暗号用セッション鍵Ｋｄを共有することができる

なお、ステップ９０４において端末２００からカード１００に伝えられるファイル名は、カードアプリケーションが管理するファイルを直接示すものである必要はなく、カードアプリケーションがどのファイルを指しているかが認識できる形であればよい。

また、端末２００がアクセスしたいファイル及びステップＳ９０５４において、そのファイルに対して端末２００がアクセス可能となる設定を行った際に割り当てられるエリア番号が常に同じとなるようにし、これらの情報を端末２００とカード１００間であらかじめ認識しておくことで、ステップ９０４における端末２００がアクセスしたいファイル名の通知およびステップ９０６におけるファイルに割り当てられたエリア番号の通知を省略することもできる。

さらに、本説明では、各カードアプリケーションが図１２で示すようにディレクトリとファイルからなる階層構造をもち、ディレクトリ名およびファイル名でデータを管理している形態で説明したが、カードアプリケーションに割り当てられた領域を適当な大きさに分割し、分割されたそれぞれの領域に番号のような識別子を割り当てて管理する形態でもよい。その場合は、図１３で示し

た処理手順で用いられるファイル名ＦＩＬＥ３の代わりに前記識別子を用いる。

次に、端末２００からセキュリティ保護領域に対してアクセスを行う際の処理について図１７及び図３を用いて説明する。図１７の実線はＣＭＤライン２２、点線はＤＡＴ０ライン２７における転送を表す。

まず、端末２００はカード１００に対してメモリカードコマンドであるアクセス領域指定コマンドを送信する（ステップ１３０１）。このアクセス領域指定コマンドは、図９で示されるフォーマットとなっており、６ビットのコマンドコード４０１と３２ビットのコマンド引数４０２から構成される。

アクセス領域指定コマンドにおけるコマンド引数４０２は、図１８で示すように、ＤＡＴ０ライン２７に入力するデータがアクセス領域指定情報であることを示すフラグ１４０１と送信データ数を示す１４０３とからなる。フラグ１４０１及び送信データ数１４０３を合わせて３２ビットに満たない場合は未使用フィールド１４０２が存在する。

ＤＡＴ０ライン２７に入力するデータは、５１２バイト単位となっており、送信データ数１４０３は、この５１２バイト単位の入力を何回行うかを示す。

次に、カード１００のコマンド受信部１０１は、端末２００から送信されたコマンドを受信し、それがアクセス領域指定コマンドであることを認識し、端末にレスポンスを返すとともにデータ制御部１０３に対して、アクセス領域指定コマンドを受信したことを通知する（ステップ１３０２）。

次に、端末２００はカード１００のＣＭＤライン２２からアクセス領域指定コマンドに対するレスポンスを受信し、ＤＡＴ０ライン２７に図２１で示すフォーマットでアクセス領域指定情報１７０２を入力する（ステップ１３０３）。

図２１の１７０１で示される長さは、後に続くアクセス領域指定情報１７０２の長さを示している。長さフィールド１７０１とアクセス領域指定情報１７０２の合計長に合わせてコマンド引数４０２の送信データ数１４０３が設定されている。また、前記合計長は必ずしも５１２バイトの倍数になるわけでは

ないので、５１２バイトの倍数になるようにパディング１７０３を付加する。

アクセス領域指定情報１７０２は、図２２で示されるように、図１３のステップ９０６でカードから通知されたエリア番号Ｘを指定するエリア番号１８０１と、０以上であり、同じくカードから通知されたファイルサイズＳＩＺＥ３の範囲で選択可能なアクセス開始アドレス１８０２と、１以上であり、（ファイルサイズＳＩＺＥ３−アクセス開始アドレス１８０２）の範囲で選択可能なアクセスデータサイズ１８０３とで構成される。

次に、カード内部のデータ送受信部１０２は、端末から入力されたアクセス領域指定情報１７０２を受信するとともに、データ制御部１０３にアクセス領域指定情報１７０２を受信したことを通知する。

次に、データ制御部１０３は、データ送受信部１０２からアクセス領域指定情報１７０２を読み出し、エリア番号１８０１が、図１５のステップＳ９０５４にて割り当てられたエリア番号Ｘであるか、アクセス開始アドレス及びアクセスデータサイズは、エリア番号Ｘと対応したファイルのファイルサイズ範囲に収まっているかをチェックし、異常があればカード内部に保持するエラーフラグをＯＮに設定する。

データ制御部１０３は、異常がなければ、図３に示すパラメータ記憶部１０９にアクセス領域指定情報１７０２（具体的にはエリア番号１８０１、アクセス開始アドレス１８０２、アクセスデータサイズ１８０３）を記憶する。

以上が、アクセス領域を指定する処理である。

次に、図１０のセキュリティ保護領域６１に対して読み出しを行う際の処理について説明する。

図１７において、端末２００は、カード１００に対してセキュリティ保護領域読み出しコマンドを送信する（ステップ１３０４）。このセキュリティ保護領域読み出しコマンドは、図８で示されるフォーマットとなっており、６ビットのコマンドコード４０１と３２ビットのコマンド引数４０２から構成される。

セキュリティ保護領域読み出しコマンドにおけるコマンド引数４０２は、セキュリティ保護領域読み出しコマンドを送信した端末が、アクセス領域指定コマンドを送信した端末２００と同一であるか、またセッション鍵共有手順を経てエリア番号Ｘが示す領域に対するアクセス権限があることを確認された端末２００と同一であるかを検証するための検証データからなる。

この検証データの生成方法について図２３を用いて説明する。

アクセス領域指定情報１７０２は、アクセス領域指定コマンドにおいてＤＡＴライン２７に入力するパラメータである。検証鍵２１０１は、図１３のステップ９０７で生成した検証用セッション鍵Ｋｍである。

端末２００内部の検証データ生成部２０３は、暗号演算を行うモジュールであり、セキュリティ保護領域アクセス（読み出しまたは書き込み）コマンドに含める検証データを生成する。ここでは、ＤＥＳ−ＭＡＣと呼ばれるＭＡＣ（Message Authentication Code）生成処理を行う。アクセス領域指定情報１７０２に対してパディングデータ２１０５を付加した２１０２を入力データとして、検証鍵２１０１を用いてＤＥＳ暗号を用いたＭＡＣ生成処理を行い、ＭＡＣデータを検証データ２１０４として作成する。

パディングデータ２１０５については、端末２００からカード１００に対してアクセス領域指定コマンドを送信するときにアクセス領域指定情報１７０２と併せて送信してもよいし、あらかじめ端末とカードの間で取り決めをしたパディング生成ルールに基づいて生成したパディングデータを付与してもよい。

なお、本実施の形態ではＤＥＳ−ＭＡＣを用いて検証データを作成しているが、他のアルゴリズムを用いてもよい。さらに、用途に応じて検証アルゴリズムを選択可能としても良い。

なお、端末２００が正当であるか認証する必要がなく、アクセス領域指定コマンドとの対応付けのみ確認したい場合は、暗号処理を用いずに、単にＳＨＡ１（Secure Hash Algorithm １）やＭＤ５（Message Digest 5）アルゴリズム

を用いたハッシュデータを検証データとして用いてもよい。

端末２００は、上記の検証データ生成処理によって３２ビットの検証データを生成し、セキュリティ保護領域読み出しコマンドの引数として使用する。

次に、カード１００のコマンド受信部１０１は、端末２００から送信されたコマンドを受信し、それがセキュリティ保護領域読み出しコマンドであることを認識し、アクセス領域指定情報１７０２に関するエラーフラグがＯＮに設定されている場合は、レスポンスとしてエラーを返す。また、アクセス領域指定情報１７０２に関するエラーフラグがＯＮに設定されていない場合は、図１５で示すように、端末に正常レスポンスを返す（ステップ１３０５）とともに、データ制御部１０３に対してセキュリティ保護領域読み出しコマンドを受信したことを通知し、パラメータ検証部１０８にコマンド引数４０２として与えられた検証データ２１０４を渡す。

次に、端末２００は、カード１００のＣＭＤライン２２からセキュリティ保護領域読み出しコマンドに対するレスポンスを受信し、ＤＡＴ０ライン２７からデータが出力されるのを待つ。

以降にカード１００によるセキュリティ保護領域のデータ出力処理について説明する。

カード１００のパラメータ検証部１０８は、パラメータ記憶部１０９からアクセス領域指定コマンドによって端末２００から与えられ、記憶しておいたアクセス領域指定情報１７０２を読み出し、アクセス領域指定情報１７０２に含まれるエリア番号Ｘ（１８０１）に対応する、図１５のステップＳ９０５９で記憶した検証用セッション鍵Ｋｍをエリア・セッション鍵管理部１１１から取得する。

次に、カード１００のパラメータ検証部１０８は、検証用セッション鍵Ｋｍとアクセス領域指定情報１７０２を用いて、図２４に示した検証データ生成処理を行い、検証データ１９０４を生成する。なお、検証データ生成処理については、図２３で示した端末２００による検証データ生成処理と同様であるので

詳細な説明は省略する。

次に、カード１００のパラメータ検証部１０８は、上記検証データ生成処理で生成した検証データ１９０４と、端末２００からセキュリティ保護領域読み出しコマンドの引数によって与えられた検証データ５０４を比較し、一致しなければエラーとし、データ読み出し処理に移行しない。一致した場合は、次のデータ読み出し処理に移行することをデータ制御部１０３に通知する。

次に、カード１００のデータ制御部１０３は、パラメータ記憶部１０９からアクセス領域指定情報１７０２を読み出し、その中に含まれるエリア番号Ｘを取得し、エリア・セッション鍵管理部１１１からエリア番号に対応するファイルＦＩＬＥ３を認識する

次に、カード１００のデータ制御部１０３は、ファイルＦＩＬＥ３がアプリケーションＡＰ１用の領域であることを確認し、格納用暗号鍵Ｋｓ＿１を取得する。

次に、カード１００のデータ制御部１０３は、アクセス領域指定情報１７０２からアクセス開始アドレス１８０２とアクセスデータサイズ１８０３を取得し、ファイルＦＩＬＥ３として管理されている領域に対して、アクセス開始アドレス１８０２をオフセット、アクセスデータサイズ１８０３を読み出しサイズとしてメモリアクセス部１０４にデータ読み出し要求を行う。

次に、カード１００のデータ制御部１０３は、暗復号部１０７に対して、メモリアクセス部１０４によって読み出されたデータを格納用暗号鍵Ｋｓ＿１で復号化するよう要求する。

次に、カード１００のデータ制御部１０３は、暗復号部１０７に対して、暗復号部１０７によって復号化されたデータを暗号用セッション鍵Ｋｄで暗号化するよう要求する。

次に、カード１００のデータ制御部１０３は、データ送受信部１０２に対して、暗復号部１０７によって暗号用セッション鍵Ｋｄで暗号化されたデータを端末２００に送信するよう要求する。

上記の処理によって、カード１００からセキュリティ保護領域のデータがセッション鍵Ｋｄによって暗号化された状態で出力可能となる。

端末２００は、カード１００からデータが出力可能となったことを認識し、図１７に示すように、ＤＡＴ０ライン２７からセッション鍵Ｋｄによって暗号化された状態のデータを取得し（ステップ１３０６）、端末が保持する暗号用セッション鍵Ｋｄによってデータを復号化し、アクセス領域指定情報１７０２で指定した領域のデータを得る。

次に、セキュリティ保護領域に対して書き込みを行う際の処理について、図２５を参照して説明する。

端末２００からのアクセス領域指定コマンドの送信（ステップ２００１）、前記コマンドに対するカード１００からのレスポンス（ステップ２００２）、及びアクセス領域指定情報の送信（ステップ２００３）については、それぞれ図１７に示したセキュリティ保護領域に対する読み出し処理におけるステップ１３０１～１３０３と同様であるので、説明を省略する。ステップ２００１～ステップ２００３を行った後、端末２００は、カード１００に対してセキュリティ保護領域書き込みコマンドを送信する（ステップ２００４）。このセキュリティ保護領域書き込みコマンドは、図８で示されるフォーマットとなっており、６ビットのコマンドコード４０１と３２ビットのコマンド引数４０２から構成される。

セキュリティ保護領域読み出しコマンドにおけるコマンド引数４０２は、セキュリティ保護領域読み出しコマンドを送信した端末２００が、アクセス領域指定コマンドを送信した端末２００と同一であるか、また、セッション鍵共有手順を経てエリア番号Ｘが示す領域に対するアクセス権限があることを確認された端末２００と同一であるかを検証するための検証データ１９０４からなる。

この検証データの生成方法についてはセキュリティ保護領域読み出しコマンドと同様であるため、詳細な説明は省略する。

端末２００は、検証データ生成処理によって３２ビットの検証データを生成し、セキュリティ保護領域書き込みコマンドの引数として使用する。

次に、カード１００のコマンド受信部１０１は、端末２００から送信されたコマンドを受信し、それがセキュリティ保護領域書き込みコマンドであることを認識し、アクセス領域指定情報１７０２に関するエラーフラグが設定されている場合は、レスポンスとしてエラーを返す。

また、アクセス領域指定情報１７０２に関するエラーフラグが設定されていない場合は、ＣＭＤライン２２から端末２００に対して正常レスポンスを返す（ステップ２００５）とともに、データ制御部１０３に対してセキュリティ保護領域書き込みコマンドを受信したことを通知し、パラメータ検証部１０８にコマンド引数として与えられた検証データ５０４を渡す。

次に、端末２００は、カード１００のＣＭＤライン２２からセキュリティ保護領域書き込みコマンドに対するレスポンスを受信し、ＤＡＴ０ライン２７にデータの入力を行う。ここでＤＡＴ０ライン２７に入力するデータは、図１３のステップ９０７で生成した暗号用セッション鍵Ｋｄで暗号化したものである。また、入力データサイズは、アクセス領域指定情報１７０２で指定したアクセスデータサイズと同一である。

以降にカードによるセキュリティ保護領域へのデータ格納処理について説明する。

カード１００のパラメータ検証部１０８は、パラメータ記憶部１０９からアクセス領域指定コマンドによって端末２００から与えられ、記憶しておいたアクセス領域指定情報１７０２を読み出し、アクセス領域指定情報１７０２に含まれるエリア番号Ｘ（１８０１）に対応する、図１５のステップ９０５９で記憶した検証用セッション鍵Ｋｍをエリア・セッション鍵管理部１１１から取得する。

次に、カード１００のパラメータ検証部１０８内部の検証データ生成部１９０３は、検証用セッション鍵Ｋｍとアクセス領域指定情報１７０２を用いて、

図２４に示した検証データ生成処理を行い、検証データ１９０４を生成する。なお、検証データ生成処理については、図２３で示した端末による検証データ生成処理と同様であるので詳細な説明は省略する。

次に、カード１００のパラメータ検証部１０８は、上記で生成した検証データ１９０４と、端末２００からセキュリティ保護領域書き込みコマンドの引数によって与えられた検証データ２１０１を比較し、一致しなければエラーとし、データ書き込み処理に移行しない。一致した場合は次のデータ書き込み処理に移行することをデータ制御部１０３に通知する。

次に、カード１００のデータ制御部１０３は、パラメータ記憶部１０９からアクセス領域指定情報１７０２を読み出し、その中に含まれるエリア番号Ｘを取得し、エリア・セッション鍵管理部１１１からエリア番号に対応するファイルＦＩＬＥ３を認識する。

次に、カード１００のデータ送受信部１０２は、端末２００から入力されたデータを受信する。

次に、カード１００のデータ制御部１０３は、ファイルＦＩＬＥ３がアプリケーションＡＰ１用の領域７１の中に存在することから、アプリケーションＡＰ１用領域７１に対応した格納用暗号鍵Ｋｓ＿１を取得する。

次に、カード１００のデータ制御部１０３は、暗復号部１０７に対して、データ送受信部１０２が受信したデータを暗号用セッション鍵Ｋｄで復号化するよう要求する。

次に、カード１００のデータ制御部１０３は、暗復号部１０７に対して、暗復号部１０７が復号化したデータを格納用暗号鍵Ｋｓ＿１で暗号化するよう要求する。

次に、カード１００のデータ制御部１０３は、アクセス領域指定情報１７０２からアクセス開始アドレス１８０２とアクセスデータサイズ１８０３を取得し、ファイルＦＩＬＥ３として管理されている領域に対し、アクセス開始アドレス１８０２をオフセット、アクセスデータサイズ１８０３を書き込みサイ

ズとして、メモリアクセス部１０４に対してデータ書き込み要求を行う。

上記のようにして、端末２００が入力したセッション鍵Ｋｄで暗号化されたデータを格納鍵Ｋｓ＿１で暗号化してフラッシュメモリ１０５に格納する。

本実施の形態では、セッション鍵の共有と、アクセス可能領域に関する情報の共有を１つのコマンドで同時に行っているが、別コマンドとして行ってもよい。

本実施の形態では、セッション鍵の共有と、アクセス可能領域に関する情報の共有を１つのコマンドで同時に行っているが、別コマンドとして行ってもよい。

以上、本発明のように、ＩＣカード用コマンドとメモリアクセス用コマンドを受信可能なメモリカードにおいて、カードアプリケーションが利用し、通常はカードアプリケーション経由でのみアクセス可能であり、端末からのアクセスが制限されているセキュリティ保護領域に対して、カードアプリケーションと端末が相互認証し、カードアプリケーションがアクセス可能設定を行うことにより、端末からメモリアクセス用コマンドを用いてアクセスすることが可能となる。

また、カードアプリケーションがアクセス可能設定を行うためのカードアプリケーションと端末間の相互認証は、用途が限定されたメモリアクセス用コマンドではなく、ＩＣカード用コマンドを使うことにより、データのセキュリティレベルに応じて相互認証方式を柔軟に選択可能となる。

また、メモリアクセス用コマンドに含められる引数サイズが３２ビットのように小さい場合でも、本発明のように、アクセス領域指定とセキュリティ保護領域アクセスのコマンドを分離し、セキュリティ保護領域アクセス用のコマンドに検証データを含めることで、アクセス領域指定を行った端末アプリケーションとセキュリティ保護領域アクセス用コマンドを発行した端末アプリケーションと検証用鍵を保持した端末アプリケーションが同一であることをカードが検証することが可能となる。

また、検証用及び暗号用セッション鍵の共有処理をセキュリティ保護領域アクセスのたびに行うことにより、セキュリティ保護領域アクセスに含める検証データとして適当な値を設定して繰り返し不正アクセスを行う攻撃に対する防御性を高めることができる。

また、端末からアクセスしたいファイルをカードに通知し、それにエリア番号を割り当て、カードから端末に通知することにより、端末がアクセス可能な領域を設定することが可能となる。また、複数のファイルに対して行うことにより、同時に複数のファイルに対してアクセス可能な状態を作ることができる。

（実施の形態２）

本実施の形態では、端末が、領域指定コマンドで指定するエリア番号をあらかじめ認識している場合のシーケンスを説明する。

まず、カード内モジュール構成について図２６を用いて説明する。なお、図２６のカード５００の端子構成は、図４に示したものと同様であるため、その図示及び説明は省略する。

カード５００内モジュールは、ＣＭＤラインに接続され、コマンドの受信及びレスポンスの送信を行う処理命令受信手段５０１と、データを格納する記憶領域５０６と、記憶領域５０６へのアクセス処理を行う記憶領域アクセス手段５０５と、ＤＡＴラインに接続され、記憶領域アクセス手段５０５が読み出したデータを外部機器に送信するデータ送信手段５０２と、同じくＤＡＴラインに接続され、外部機器からデータを受信するデータ受信手段５０３と、処理命令受信手段５０１が受け取った指定情報を検証する指定情報検証手段５０４と、からなる。

次に、端末６００内モジュール構成について、図２７を用いて説明する。

端末６００内モジュールは、カード５００に対するコマンド送信と、レスポンス受信を行う処理命令送信手段６０４と、カード５００に対するデータ送信を行うデータ送信手段６０５と、カード５００からのデータ受信を行うデータ受信手段６０６と、アクセスする領域を決定する指定情報決定手段６０１と、指定情

報から検証情報を生成する検証情報生成手段６０２と、カード５００に送信するデータ及びカード５００から受信するデータを格納するデータ記憶手段６０３と、からなる。

次に、端末６００からカード５００のセキュリティ保護領域に対してアクセスを行う際の処理について、上記図２６及び図２７と、図２８に示すフローチャートを用いて説明する。

まず、端末６００は指定情報決定手段６０１にてリードアクセス又はライトアクセスを行う領域を決定し（ステップＳ２６０１）、アクセス領域指定情報を生成する（ステップＳ２６０２）。次に、このアクセス領域指定情報をデータ記憶手段６０３に格納して領域指定命令を処理命令送信手段６０４からカード５００に送信する（ステップＳ６０３）。

領域指定命令のデータ部の一例を図２９に示す。

ＤＡＴライン２７に入力するデータは５１２バイト単位となっており、領域指定命令のデータ部は、アクセス領域指定情報２７０２の長さフィールド２７０１と、アクセス領域指定情報フィールド２７０２の合計長が５１２バイトに満たない場合、パディング２７０３が追加される。本実施の携帯では、長さフィールド２７０１は２バイトの長さを持ち、アクセス領域指定情報２７０２は、図３０に示すように、１バイトのエリア番号２８０１、３バイトのアクセス開始アドレス２８０２、及び３バイトのアクセスデータサイズ２８０３からなる。つまり合計９バイトであり５１２バイトに満たないため、５０３バイトのパディング２７０３が付加される。

次に、図２８に戻り、カード５００は、処理命令受信手段５０１にて領域指定命令を受信すると（ステップＳ２６０４）、指定情報検証手段５０４にてアクセス領域指定情報２７０２を確認し、指定した領域が正しいかどうかをエリア番号２８０１に対応する領域が存在するか、アクセス開始アドレス２８０２及びアクセスデータサイズ２８０３がエリア番号２８０１で示された領域の範囲に収まっているかを元に判断する（ステップＳ２６０５）。指定情報検証

手段５０４は、指定した領域が正しくなければ、領域指定命令を無効として扱う（ステップＳ２６０６）。指定した領域が正しい場合、アクセス領域指定情報２７０２を保存し、アクセス領域指定情報２７０２と、端末６００とカード５００の間で共有している鍵を用いて、比較情報を生成する（ステップＳ２６０７）。

比較情報の生成方法の一例を図２９に示す。

検証データ生成部２９０２は暗号演算を行うモジュールであり、本実施の形態ではＤＥＳ－ＭＡＣと呼ばれるＭＡＣ（Message Authentication Code）を生成する処理を行う。入力は、領域指定命令のデータ部２７０４と、端末６００との間で共有している検証用の鍵２９０１である。ＤＥＳ－ＭＡＣの出力結果は６４ビットであるが、本実施の形態では、比較対象となる端末６００から送信される検証情報が３２ビットであるため、その出力を切り詰めた２９０３である前半３２ビットのみを比較情報２９０４として用いる。なお、検証用鍵２９０１は、エリア番号に対応して個別かつ固定の鍵であってもよいし、エリア番号によらず１つの鍵であってもよい。

また、図３２に示すように、カード７００内部に検証用鍵共有手段７０１を備え、図３３に示すように端末８００内部に検証用鍵共有手段８０１を備え、カード７００と端末８００の間で、セキュリティ保護領域へのアクセスを行うたびに検証用鍵を変更してもよい。なお、図３２及び図３３の各構成において、図２６及び図２７に示した構成と同一部分には同一符号を付している。

次に、検証用鍵の共有方法について上記図３２及び図３３と、図３４に示すシーケンスおよび図３５に示す検証用鍵生成方法を用いて説明する。

図３４において、端末８００は検証用鍵共有手段８０１において、乱数Ｒａを生成し、この乱数Ｒａを含んだセッション鍵共有要求コマンドＡＰＤＵを作成し、処理命令送信手段６０４からＡＰＤＵ送信コマンドをカード７００に送信するとともに（ステップＳ３２０１）、データ送信手段６０５からセッション鍵共有要求コマンドＡＰＤＵをカード７００に送信する（ステップＳ３２０

２）。

次に、カード７００は処理命令受信手段５０１にてＡＰＤＵ送信コマンドを端末８００から受信し、データ受信手段５０３にて端末８００から受信したセッション鍵共有要求コマンドＡＰＤＵを検証用鍵共有手段７０１に渡す。

検証用鍵共有手段８０１では、乱数Ｒｂを生成し、図３５に示すように、端末８００から受信した乱数Ｒａと乱数Ｒｂを結合したものに対し、あらかじめ端末８００との間で共有しているマスター鍵Ｋを用いて暗号化処理（ＤＥＳ－ＭＡＣ処理）を行い、セッション鍵Ｒを生成する。次に、カード７００は、乱数Ｒｂを含むレスポンスＡＰＤＵを生成する。

次に、端末８００は、処理命令送信手段６０４からＡＰＤＵ受信コマンドをカード７００に送信する（ステップＳ３２０３）。

次に、カード７００は、処理命令受信手段５０１にてＡＰＤＵ受信コマンドを端末８００から受信し、先ほど作成した乱数Ｒｂを含むレスポンスＡＰＤＵをデータ送信手段５０２より端末８００に送信する（ステップＳ３２０４）。

次に、端末８００は、データ受信手段６０６によりレスポンスＡＰＤＵをカード７００から受信し、検証用鍵共有手段８０１に渡す。検証用鍵共有手段８０１は、図３５に示すように、先ほど自身が生成した乱数Ｒａと、レスポンスＡＰＤＵに含まれる乱数Ｒｂを結合したものに対し、あらかじめカード７００との間で共有しているマスター鍵Ｋを用いて暗号化処理(DES－MAC処理)を行い、セッション鍵Ｒを生成する。

以上が、セキュリティ保護領域へのアクセスを行うたびにセッション鍵を変更する場合の、端末８００とカード７００の間における検証用鍵共有手順である。

なお，本実施の形態ではＤＥＳ－ＭＡＣを用いているが、当然他の暗号アルゴリズムを用いてもよい。また、端末８００が正当であるか、つまり同一の鍵を持っているかを検証する必要がない場合、例えば、領域指定命令のアクセス領域指定情報２７０２が端末の意図したものになっているかの検証のみ行う

場合は、暗号処理を用いずに、図３６に示すような検証データ生成部３４０１にてＳＨＡ－１演算や、ＭＤ５アルゴリズムを用いたハッシュ演算やチェックサム演算の結果を比較情報として用いることができる。これらのアルゴリズムを用いた場合も、比較対象が３２ビット長ならば、出力結果を切りつめ３４０２、その一部の３２ビットのみを比較情報３４０３とする。

次に、図２８に戻り、端末８００は、検証データ生成部にてアクセス領域指定情報２７０２と、端末８００とカード７００の間で共有している検証用鍵２９０１から検証情報を生成する（ステップＳ２６０８）。

この検証情報の生成について、図３７に示す。検証情報生成部３５０２にて検証用鍵３５０１と領域指定命令のデータ部２７０４を用いて暗号処理を行い、検証情報３５０４を生成する。生成方法は、図３１で示したカード７００における比較情報２９０４の生成方法と全く同じである。

次に、図２８に戻り、端末８００は、生成した検証情報３５０４をアクセス命令（読み出し）の引数に載せて、処理命令送信手段６０４からアクセス命令を送信する（ステップＳ６０９）。

アクセス命令は、図３８で示すフォーマットとなっており、コマンドコード３６０１とコマンド引数３６０２の長さはそれぞれ６ビットと３２ビットである。アクセス命令では、コマンド引数３６０２に検証情報３５０４を格納する。

次に、図２８に戻り、カード７００は、処理命令受信手段５０１にてアクセス命令（読み出し）を受信し（ステップＳ２６１０）、指定情報検証手段５０４にて事前に領域指定命令が正常に完了したかどうかを確認する（ステップＳ２６１１）。領域指定命令が未受信である、又は指定した領域が正しくないなどの理由で正常に完了していない場合は、アクセス命令をエラーとして端末８００に通知する（ステップＳ２６１２）。この時、端末８００は、カード７００からエラーを受信する（ステップＳ２６１２Ａ）。

事前に領域指定命令が正常に完了している場合、指定情報検証手段５０４は、

先ほどカード７００が作成した比較情報２９０４と、アクセス命令のコマンド引数に格納された検証情報３５０４を比較する（ステップＳ２６１３）。比較の結果、検証情報３５０４が不正であったならば、アクセス命令をエラーとして端末８００に通知する（ステップＳ２６１４）。この時、端末８００は、カード７００からエラーを受信する（ステップＳ２６１４Ａ）。検証情報が正常であったならば、指定情報検証手段５０４４は記憶領域アクセス手段５０５にアクセス領域指定情報２７０２を通知し、記憶領域アクセス手段５０５は記憶領域５０６内のアクセス領域指定情報２７０２で指定された領域からデータを読み出し、データ送信手段５０２からデータを端末８００に送信する（ステップＳ２６１５）。

次に、端末８００は、カード７００から送信された読み出しデータをデータ受信手段６０６にて受信し（ステップＳ２６１６）、データ記憶手段６０３に格納する。

以上の通り、メモリアクセス用コマンドに含められる引数サイズが３２ビットのように小さい場合でも、本発明のように、アクセス領域指定とセキュリティ保護領域アクセスのコマンドを分離し、セキュリティ保護領域アクセス用のコマンドに検証データを含めることで、アクセス領域指定を行った端末アプリケーションとセキュリティ保護領域アクセス用コマンドを発行した端末アプリケーションと検証用鍵を保持した端末アプリケーションが同一であることをカードが検証することが可能となる。

なお、検証データ生成のために、領域指定情報と検証用鍵に加え、カードから出力される乱数情報を利用する方法を、図３９に示すシーケンスを用いて以下に説明する。なお、図３９に示す各ステップにおいて、図２８に示したシーケンスのステップと同一のステップには同一符号を付して、その説明は省略する。

図３９に示すように、端末８００から乱数取得命令を端末８００からカード７００に送信し(ステップＳ３７０１)、カード７００が乱数Ｔを生成し、この

乱数Ｔをカード７００内部の指定情報検証手段５０４に保持するとともに、データ送信手段５０２から端末８００に送信する（ステップＳ３７０２）。端末８００は、カード７００から送信された乱数Ｔをデータ受信手段６０６にて受信する（ステップＳ３７０３）。

乱数Ｔを検証情報生成処理に利用する場合のカード７００における比較情報の生成処理（ステップＳ２６０７）、および、端末８００における検証情報の生成処理（ステップＳ２６０８）は、それぞれ図４０および図４１で示すように、乱数Ｔと領域指定命令のデータ部２７０４を結合したものに対して暗号処理を行い、比較情報３８０４及び検証情報３９０４を出力する。

以上のように、検証情報生成に乱数情報を利用することにより、同一の領域指定情報と検証用鍵を用いて検証情報を作成しても、乱数情報が変化することで出力される検証情報が変化するため、よりセキュリティ強度を向上させることができる。

（実施の形態３）

本実施の形態では、鍵の共有処理を含むシーケンスの例を説明する。

まず、カード内モジュール構成について図４２を用いて説明する。なお、カードの端子構成は、図４に示したものと同様であるため、その図示及び説明は省略する。

カード内モジュールは、ＣＭＤラインに接続され、コマンドの受信及びレスポンスの送信を行う処理命令受信手段９０１と、データを格納する記憶領域９０６と、記憶領域９０６へのアクセス処理を行う記憶領域アクセス手段９０５と、ＤＡＴラインに接続され、記憶領域アクセス手段９０５が読み出したデータを外部機器に送信するデータ送信手段９０２と、同じくＤＡＴラインに接続され、外部機器からデータを受信するデータ受信手段９０３と、端末１０００との間でセキュリティ保護領域アクセスコマンドによるアクセスが可能な領域に関する情報を共有する可能領域情報共有部９０７と、データ受信手段９０３経由して受け取った指定情報を、検証用鍵を用いて検証する指定情報検証手

段９０４と、からなる。

次に、端末内モジュール構成について、図４３を用いて説明する。

端末内モジュールは、カード９００に対するコマンド送信と、レスポンス受信を行う処理命令送信手段１００４と、カード９００に対するデータ送信を行うデータ送信手段１００５と、カード９００からのデータ受信を行うデータ受信手段１００６と、アクセスする領域を決定する指定情報決定手段１００１と、セキュリティ保護領域アクセスコマンドによるアクセスが可能な領域に関する情報を共有する可能領域情報共有部１００７と、指定情報から検証情報を生成する検証情報生成手段１００２と、カード９００に送信するデータ及びカード９００から受信するデータを格納するデータ記憶手段１００３と、からなる。

次に、端末１０００からカード９００内のセキュリティ保護領域に対してアクセスを行う際の処理について、上記図４２及び図４３と、図４４及び図４５に示すシーケンスを用いて説明する。

まず、端末１０００は、指定情報決定手段１００１にて、リードアクセス又はライトアクセスを行う領域Ａを決定し（ステップＳ４２０１）、可能領域情報共有部１００７にて、前記領域Ａに対するセキュリティ保護領域アクセスコマンドによるアクセスを許可するように要求するコマンドＡＰＤＵである領域開放要求コマンドを処理命令送信手段１００４からカード９００に送信する（ステップＳ４２０２）。領域開放要求コマンドは、端末１０００の公開鍵を表す識別子Ｉｎｆｏ＿ＰｕｂＨと、領域Ａを示す識別子ａをカード９００の公開鍵ＰｕｂＳで暗号化したデータとを含む。なお、コマンドＡＰＤＵの送信方法は実施の形態１で説明した方法と同様であるので、詳細な説明は省略する。

次に、領域開放要求コマンドを受信したカード９００は、可能領域情報共有手段９０７にてコマンドに含まれる暗号化データをカード９００自身の秘密鍵ＰｒｉＳで復号化する（ステップＳ４２０３）。次いで、端末１０００の公開鍵識別子Ｉｎｆｏ＿ＰｕｂＨからコマンドを送信した端末１０００を識別し、識別子ａで示される領域Ａのアクセス権限を参照することで、該端末１０

００が領域Ａに対するアクセスを許可されているかどうかを確認する（ステップＳ４２０５）。

アクセスが許可されていない場合は、領域開放失敗を示すデータをレスポンスＡＰＤＵとしてデータ送信手段９０２から端末１０００に送信する（ステップＳ４２０６）。アクセスが許可されている場合は、領域Ａの識別子ａと領域Ａに割り当てたエリア番号Ｘを、指定情報検証手段９０４内に持つ、セキュリティ保護領域アクセスコマンドによるアクセス可否を設定するアクセス有効テーブル４４００（図４６参照）に登録する（ステップＳ４２０７）。次に、領域Ａに対応した検証用鍵Ｒをアクセス有効テーブル４４００に登録する（ステップＳ４２０８）。

次に、エリア番号Ｘ、領域Ａのサイズを端末１０００の公開鍵ＰｕｂＨで暗号化し、レスポンスＡＰＤＵとしてデータ送信手段９０２から端末１０００に送信する（ステップＳ４２０９）。

次に、端末１０００は、ＡＰＤＵ受信コマンドを処理命令送信手段１００４からカード９００に送信し、データ受信手段１００６を用いてレスポンスＡＰＤＵをカード９００から取得する（ステップＳ４２１０）。なお、レスポンスＡＰＤＵの取得方法は実施の形態１で説明した方法と同様であるので、詳細な説明は省略する。

次に、端末１０００の可能領域情報共有手段１００７は、レスポンスＡＰＤＵに含まれる暗号データを端末１０００自身の秘密鍵ＰｒｉＨで復号化し（ステップＳ４２１１）、エリア番号Ｘ、エリア番号Ｘで示される領域Ａのサイズを得る。次に、端末１０００は領域Ａに対応したセッション鍵を検証情報生成手段１００２に登録する。エリア番号Ｘはアクセス領域指定情報を生成するために指定情報決定手段１００１に登録する（ステップＳ４２１２）。以後、図４５のフローチャートに移行する。

次に、端末１０００は指定情報決定手段１００１にて可能領域情報共有手段１００７によって登録されたエリア番号Ｘを用いてアクセス領域指定情報を

生成する（ステップＳ４２１３）。次に、このアクセス領域指定情報をデータ部２７０４（図２９参照）に格納して、領域指定命令を処理命令送信手段１００４からカード９００に送信する（ステップＳ４２１４）。なお、領域指定命令におけるアクセス領域指定情報は実施の形態２と同様であるので、詳細な説明は省略する。

次に、カード９００は、処理命令受信手段９０１にて端末１０００から領域指定命令を受信すると（ステップＳ４２１５）、指定情報検証手段９０４にてアクセス領域指定情報を確認し、エリア番号Ｘがアクセス有効テーブル４４００に登録されているか、図３０に示したアクセス開始アドレス２８０２及びアクセスデータサイズ２８０３を元に領域Ａの範囲に収まっているか判断する（ステップＳ４２１６）。指定情報検証手段９０４は、指定した領域が正しくなければ、領域指定命令を無効として扱う（ステップＳ４２１７）。指定した領域が正しい場合、アクセス領域指定情報を保存し、アクセス領域指定情報とアクセス有効テーブル４４００に登録された領域Ａに対応した検証用鍵Ｒを用いて、比較情報を生成する（ステップＳ４２１８）。なお、比較情報の生成方法は実施の形態２と同様であるので、詳細な説明は省略する。

次に、端末１０００は、検証情報生成手段１００２にてアクセス領域指定情報と、可能領域情報共有部１００７によって登録されたセッション鍵Ｒを用いて検証情報を生成し（ステップＳ４２１９）、アクセス命令（読み出し）の引数に載せて、処理命令送信手段１００１からアクセス命令をカード９００に送信する（ステップＳ４２２０）。なお、検証情報の生成方法及びアクセス命令の送信方法は実施の形態２と同様であるので、詳細な説明は省略する。

次に、カード９００は、処理命令受信手段９０１にてアクセス命令（読み出し）を受信し（ステップＳ４２２１）、指定情報検証手段９０４にて事前に領域指定命令が正常に完了したかどうかを確認する（ステップＳ４２２２）。領域指定命令が未受信である、又は指定した領域が正しくないなどの理由で正常に完了していない場合は、アクセス命令をエラーとして端末１０００に通知す

る（ステップＳ４２２３）。この時、端末１０００は、カード９００からエラーを受信する（ステップＳ４２２３Ａ）。

事前に領域指定命令が正常に完了している場合、指定情報検証手段９０４は、先ほどカード９００が作成した比較情報と、アクセス命令の引数に格納された検証情報を比較する（ステップＳ４２２４）。比較の結果、検証情報が不正であったならば、アクセス命令をエラーとして端末１０００に通知する（ステップＳ４２２５）。この時、端末１０００は、カード９００からエラーを受信する（ステップＳ４２２５Ａ）。

検証情報が正常であったならば，指定情報検証手段９０４は、記憶領域アクセス手段９０５に指定情報を通知し、記憶領域アクセス手段９０５は記憶領域９０６内の領域指定命令で指定された領域からデータを読み出し、データ送信手段９０２からデータを端末１０００に送信する（ステップＳ４２２６）。

次に、端末１０００は、カード９００から送信された読み出しデータをデータ受信手段１００６にて受信し、データ記憶手段１００３に格納する（ステップＳ４２２７）。

次に、端末１０００は、領域Ａに対するセキュリティ保護領域アクセスコマンドによるアクセスが不要になったとき、領域Ａに対応するエリア番号Ｘを無効化するための領域無効コマンドＡＰＤＵを作成し、データ送信手段１００５からカード９００に送信する（ステップＳ４２２８）。

次に、領域無効コマンドＡＰＤＵを受信したカード９００は、アクセス有効テーブル４４００を検索し、エリア番号Ｘが見つかれば、テーブル内のエリア番号Ｘに割り当てられた領域識別子ａ、セッション鍵Ｒとともにエリア番号Ｘの登録を削除し、エリア番号Ｘを指定した領域Ａへのセキュリティ保護領域アクセスコマンドによるアクセスを無効化する（ステップＳ４２２９）。

以上の通り、セキュリティ保護領域内のある領域に対し、必要な場合のみ領域開放要求によってセキュリティ保護領域アクセスコマンドによるアクセスが可能な状態にし、また不要となったときは領域無効要求によって、その領域

へのアクセスを不可能にすることで、セキュリティ強度を向上させることができる。

本明細書は、２００３年７月１６日出願の特願２００３－２７５６７２及び２００４年７月２日出願の特願２００４－１９７４５３に基づく。この内容はすべてここに含めておく。

産業上の利用可能性

メモリカードコマンドとＩＣカードコマンドを併用し、メモリアクセスについてはメモリカードコマンドを使用することで複雑さを回避しながら、少ないコマンド引数でも安全に端末を認証可能とすることができる。

請求の範囲

1．機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法。

2．機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、前記可能領域情報を参照し、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法。

3．機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、検証用鍵を共有化するステップと、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法。

４．　機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、前記メモリデバイスとで、前記アクセス可能領域に対応した検証用鍵を共有化するステップと、前記可能領域情報を参照し、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法。

５．　機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、第一の処理系コマンドを用いて、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、前記可能領域情報を参照し、第二の処理系コマンドを用いて、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法。

６．　機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスとで、第一の処理系コマンドを用いて、検証用鍵を共有化するステップと、第二の処理系コマンドを用いて、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、

前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法。

7． 機器からメモリデバイスに対するアクセス方法であって、前記メモリデバイスは、前記機器からのアクセスが制約された耐タンパ性の第1領域と、前記機器からのアクセスが制約された非耐タンパ性の第2領域と、前記機器からアクセスすることが可能な第3領域と、を有し、少なくとも前記第1領域への処理命令である第一の処理系コマンドと、少なくとも前記第3領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、前記機器は、前記メモリデバイスとで、第一の処理系コマンドを用いて、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、前記可能領域情報を参照し、第二の処理系コマンドを用いて、前記第2領域へのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報と、を併せて送信するステップと、前記メモリデバイスは、前記指定情報を受信するステップと、前記処理命令と前記検証情報を受信し、前記指定情報を前記検証情報を用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法。

8． 機器からメモリデバイスに対するアクセス方法であって、前記メモリデバイスは、前記機器からのアクセスが制約された耐タンパ性の第1領域と、前記機器からのアクセスが制約された非耐タンパ性の第2領域と、前記機器からアクセスすることが可能な第3領域と、を有し、少なくとも前記第1領域への処理命令である第一の処理系コマンドと、少なくとも前記第3領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、前記機器は、前記メモリデバイスとで、第一の処理系コマンドを用いて、検証用鍵を共有化するステップと、第二の処理系コマンドを用いて、前記第2領域へのアクセス領域

を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスは、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法

９．　機器から読み書きされるメモリデバイスであって、アクセスする領域を指定する指定情報を受信するとともに、前記指定情報に基づく検証情報と読み出し又は書き込み命令を併せて受信する処理命令受信手段と、前記指定情報を、前記検証情報を用いて検証処理を行う指定情報検証手段と、データを格納する記憶領域と、前記検証処理が成功した場合に、前記処理命令に応じて、前記記憶領域の前記指定領域に対する読み出し又は書き込みを行う記憶領域アクセス手段と、前記記憶領域アクセス手段が読み出したデータを前記機器に送信するデータ送信手段と、前記機器から書き込みデータを受信するデータ受信手段と、を備えることを特徴とするメモリデバイス。

１０．　前記指定情報検証手段の検証処理が、前記検証情報と検証用鍵を用いて行うことを特徴とする請求の範囲９記載のメモリデバイス。

１１．　前記機器との間で前記検証用鍵を共有する検証用鍵共有手段をさらに備えることを特徴とする請求の範囲１０記載のメモリデバイス。

１２．　前記機器との間でメモリデバイスへのアクセス可能な領域を示す可能領域情報を共有する可能領域情報共有手段をさらに備えることを特徴とする請求の範囲９記載のメモリデバイス。

１３．　メモリデバイスを読み書きする情報機器であって、読み出し又は書き込みする領域を決定し、前記領域を指定する指定情報を決定する指定情報決定手段と、前記指定情報から前記検証情報の生成処理を行う検証情報生成手段と、前記指定情報の送信と、前記検証情報と読み出し又は書き込みの処理命令とを

併せて送信する処理命令送信手段と、前記処理命令が書き込みの場合は、前記メモリデバイスにデータを送信するデータ送信手段と、前記処理命令が読み出しの場合は、前記メモリデバイスからデータを受信するデータ受信手段と、前記メモリデバイスに送信するデータを記憶し、または、前記メモリデバイスから受信したデータを記憶するデータ記憶手段と、を備えることを特徴とする情報機器。

１４．　前記検証情報生成手段の前記検証情報の生成処理が、前記指定情報と検証用鍵とを用いて行うことを特徴とする請求の範囲１３記載の情報機器。

１５．　前記メモリデバイスとの間で前記検証用鍵を共有する検証用鍵共有手段を備えることを特徴とする請求の範囲１４記載の情報機器。

１６．　前記メモリデバイスとの間で、当該メモリデバイスへのアクセス可能な領域を示す可能領域情報を共有する可能領域情報共有手段をさらに備えることを特徴とする請求の範囲１３記載の情報機器。

１７．　機器からメモリデバイスに対するアクセス方法であって、前記機器が、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスが、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと検証用鍵とを用いて検証するステップと、前記検証に成功した場合、前記処理命令を実行するステップと、を有するアクセス方法。

１８．　機器からメモリデバイスに対するアクセス方法であって、前記機器は、第一の処理系コマンドを用いて前記メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、第一の処理系コマンドを用いて前記アクセス可能領域に対応した検証用鍵を共有化するステップと、第ニの処理系コマンドを用いて、前記メモリデバイスへのアクセス領域を指定する指定情報を送信するステップと、第ニの処理系コマンドを用いて前記アクセス領域

への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスは、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し、前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合は、前記処理命令を実行するステップと、を有するアクセス方法。

１９． 機器からメモリデバイスに対するアクセス方法であって、前記メモリデバイスは、前記機器からのアクセスが制約された耐タンパ性の第１領域と、前記機器からのアクセスが制約された非耐タンパ性かつ大容量の第２領域と、前記機器からアクセスすることが可能なかつ大容量の第３領域と、を有し、少なくとも前記第１領域への処理命令である第一の処理系コマンドと、少なくとも前記第３領域への処理命令である第二の処理系コマンドと、を判別する機能を備え、前記機器は、前記メモリデバイスとで、第一の処理系コマンドを用いて、当該メモリデバイスへのアクセス可能領域に関する可能領域情報を共有化するステップと、第一の処理系コマンドを用いて、前記アクセス可能領域に対応した検証用鍵を共有化するステップと、第二の処理系コマンドを用いて、前記第２領域へのアクセス領域を指定する指定情報を送信するステップと、第二の処理系コマンドを用いて、前記アクセス領域への処理命令と、前記指定情報に関する検証情報を前記検証用鍵で暗号化した検証データと、を併せて送信するステップと、前記メモリデバイスは、前記指定情報を受信するステップと、前記処理命令と前記検証データを受信し前記指定情報を前記検証データと前記検証用鍵とを用いて検証するステップと、前記検証にて成功した場合、前記処理命令を実行するステップと、を有するアクセス方法。

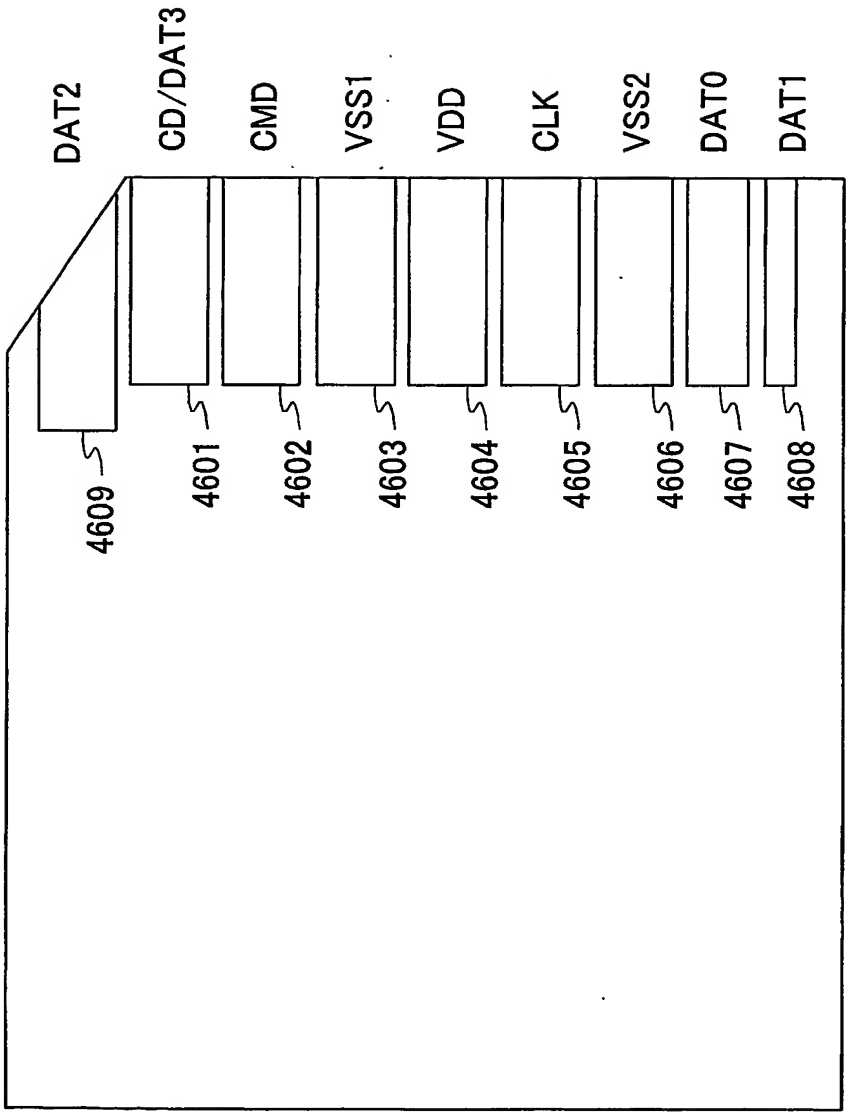

DAT2
CD/DAT3
CMD
VSS1
VDD
CLK
VSS2
DAT0
DAT1
4609
4601
4602
4603
4604
4605
4606
4607
4608

図1

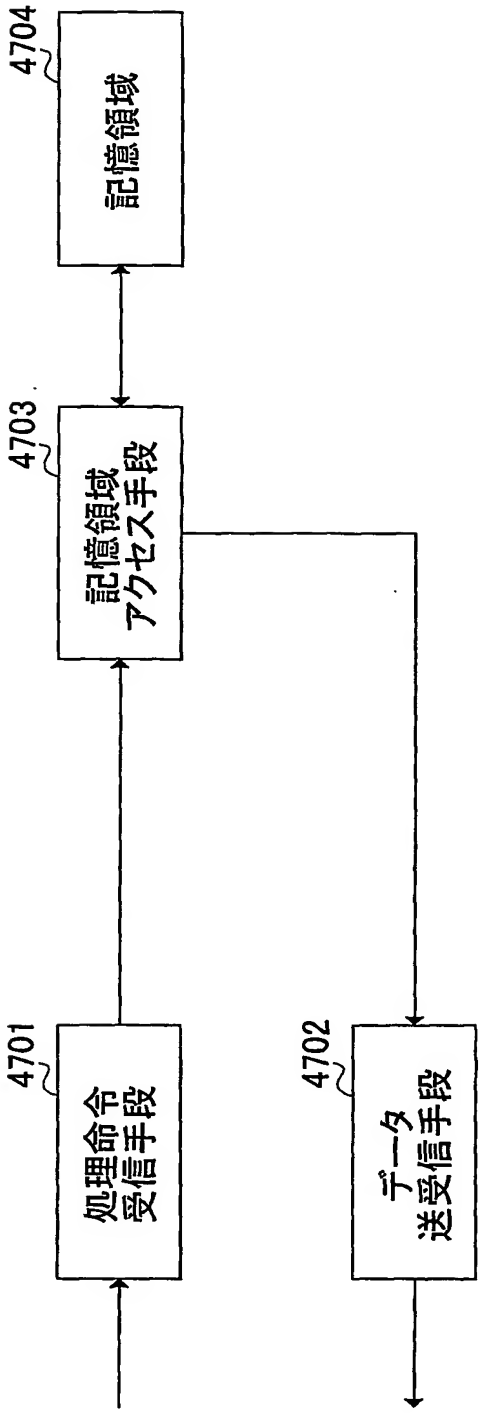


図2

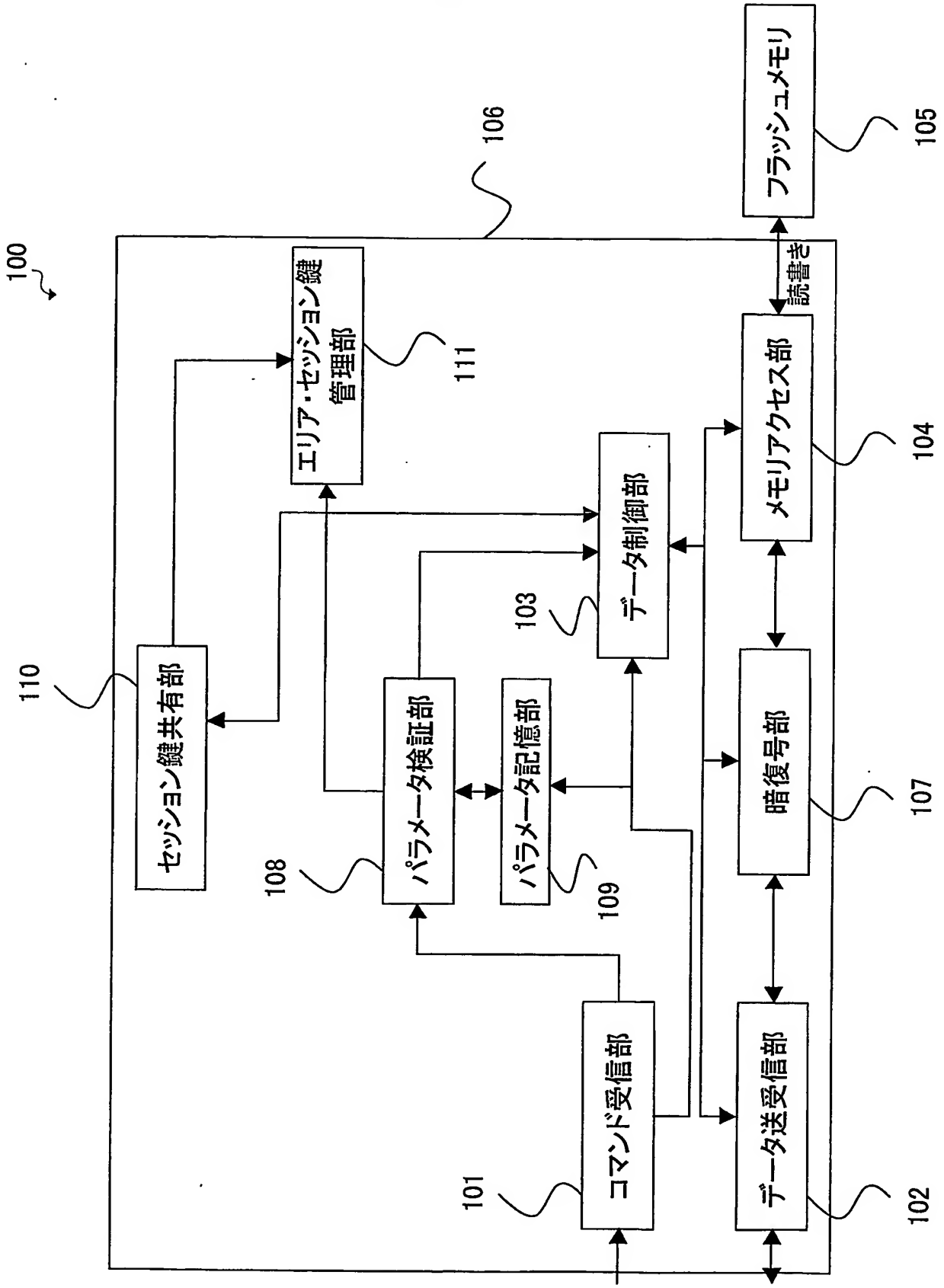

100
101
102
103
104
105
106
107
108
109
110
111
コマンド受信部
データ送受信部
データ制御部
メモリアクセス部
フラッシュメモリ
パラメータ検証部
パラメータ記憶部
暗復号部
セッション鍵共有部
エリア・セッション鍵管理部
読書き

図3

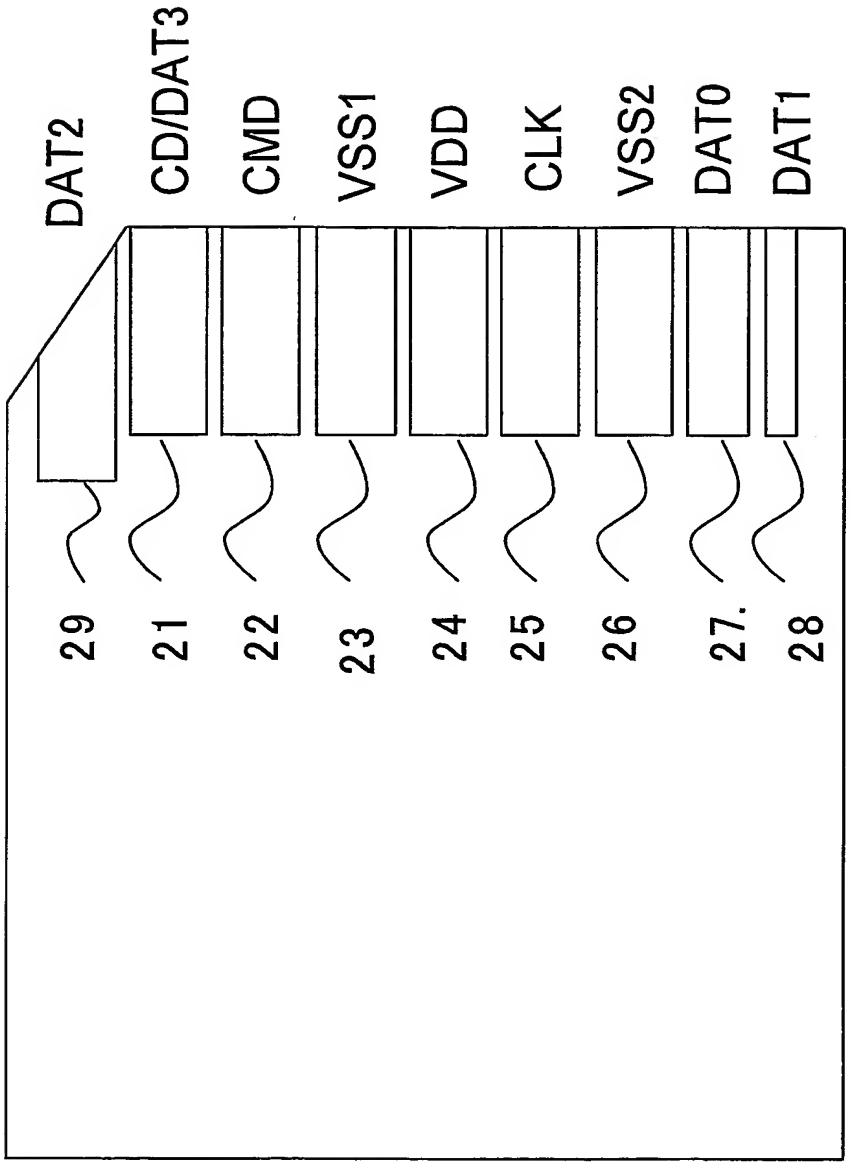

DAT2
CD/DAT3
CMD
VSS1
VDD
CLK
VSS2
DAT0
DAT1
29
21
22
23
24
25
26
27.
28

図4

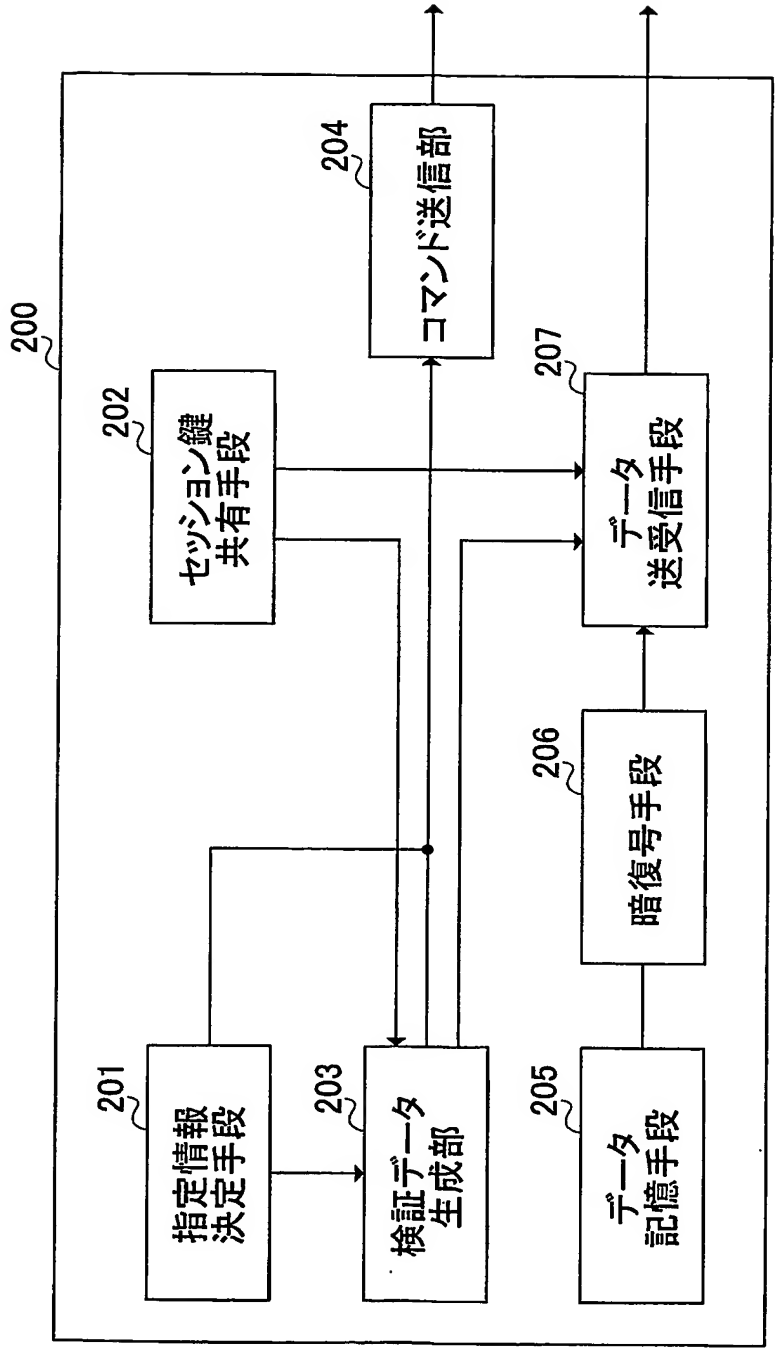

200
201
指定情報
決定手段
202
セッション鍵
共有手段
203
検証データ
生成部
204
コマンド送信部
205
データ
記憶手段
206
暗復号手段
207
データ
送受信手段

図5

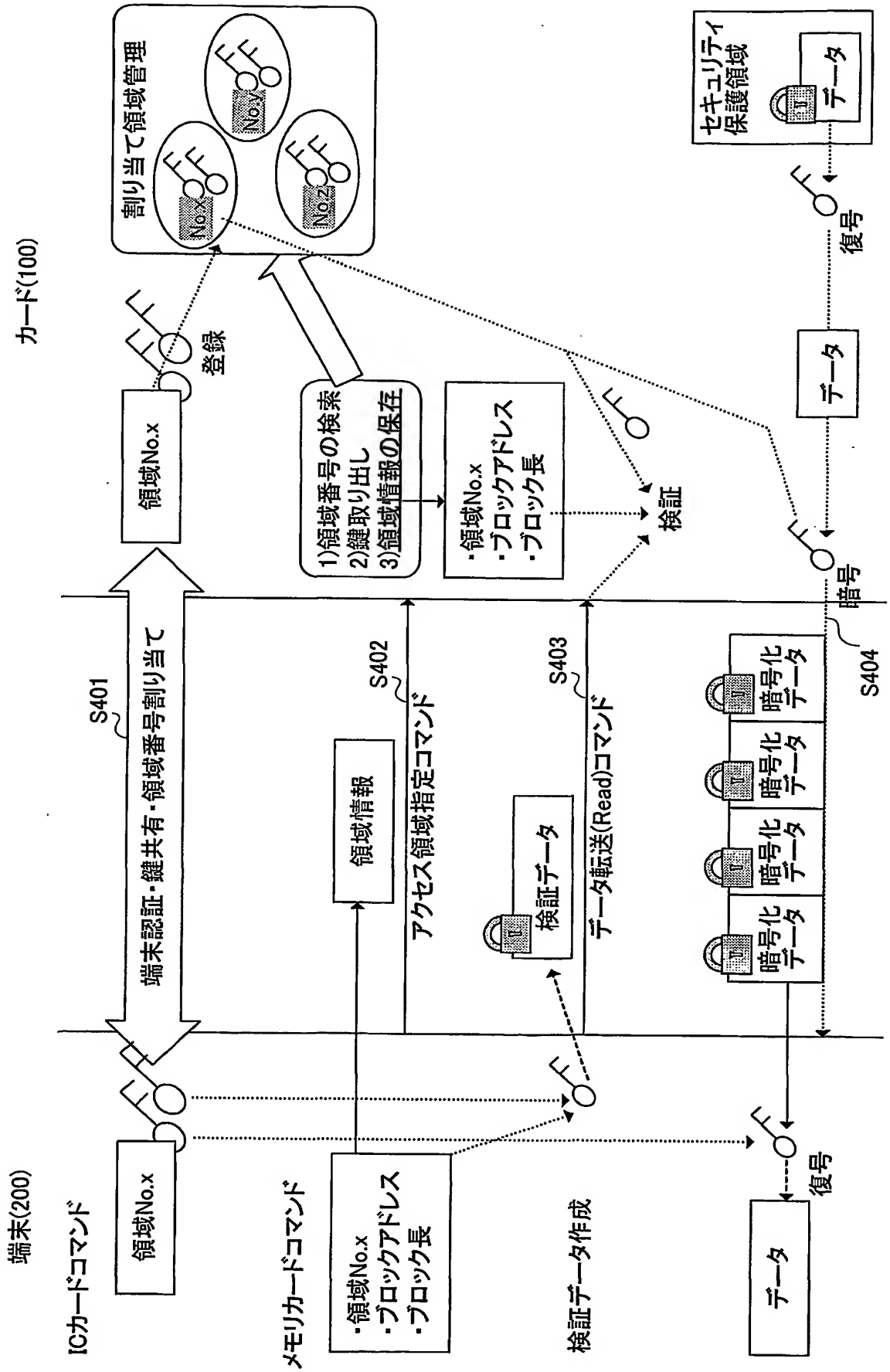

カード(100)
割り当て領域管理
No.X
No.Y
No.Z
登録
領域No.x
1)領域番号の検索
2)鍵取り出し
3)領域情報の保存
・領域No.x
・ブロックアドレス
・ブロック長
検証
セキュリティ保護領域
データ
復号
暗号
S401
端末認証・鍵共有・領域番号割り当て
S402
アクセス領域指定コマンド
S403
データ転送(Read)コマンド
S404
領域情報
検証データ
暗号化データ
端末(200)
ICカードコマンド
メモリカードコマンド
検証データ作成

図6

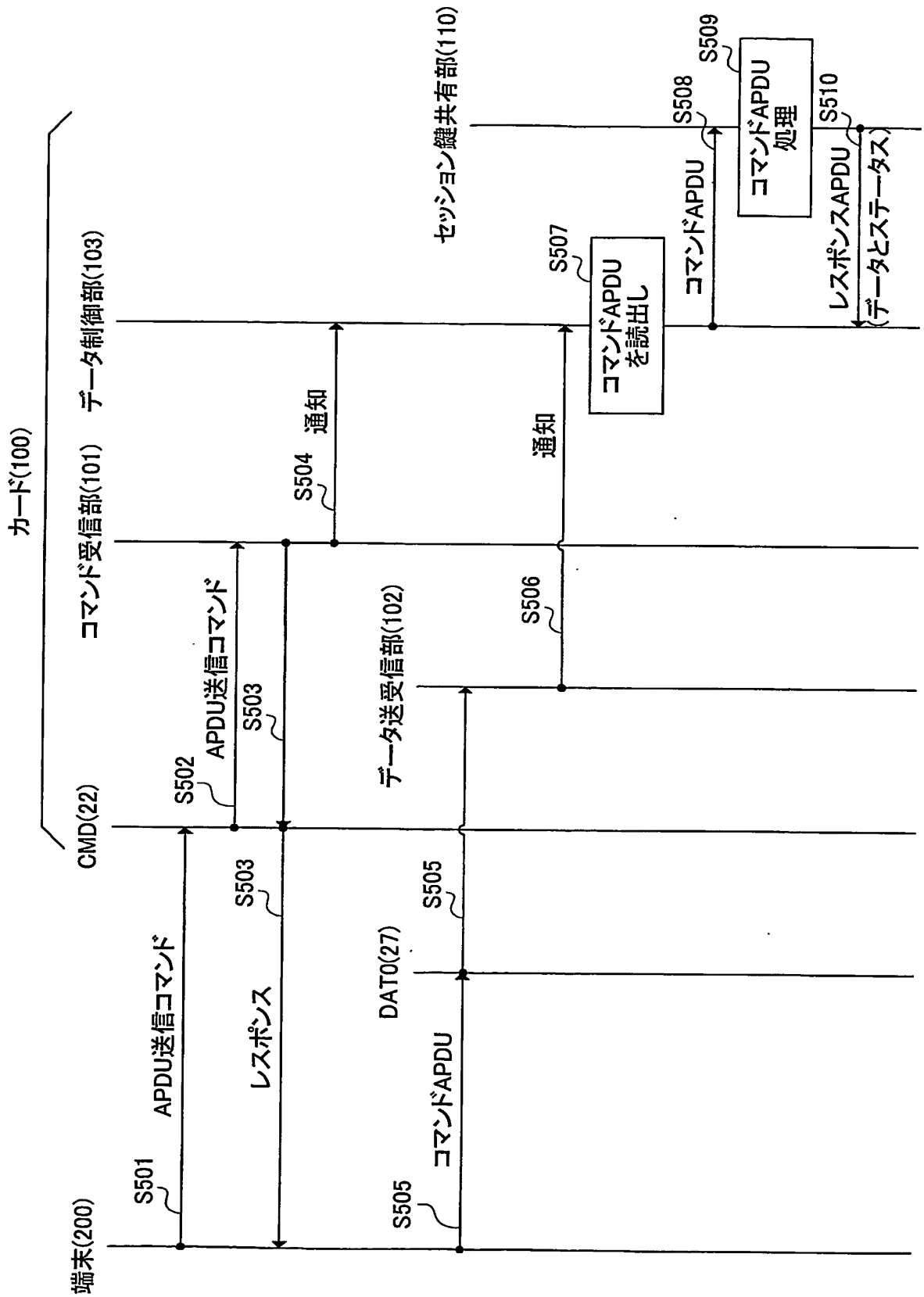

カード(100)
端末(200)
CMD(22)
コマンド受信部(101)
データ制御部(103)
データ送受信部(102)
セッション鍵共有部(110)
S501
APDU送信コマンド
S502
APDU送信コマンド
S503
レスポンス
S503
S504
通知
S505
DAT0(27)
コマンドAPDU
S505
S506
通知
S507
コマンドAPDU
を読出し
S508
コマンドAPDU
S509
コマンドAPDU
処理
S510
レスポンスAPDU
(データとステータス)

図7

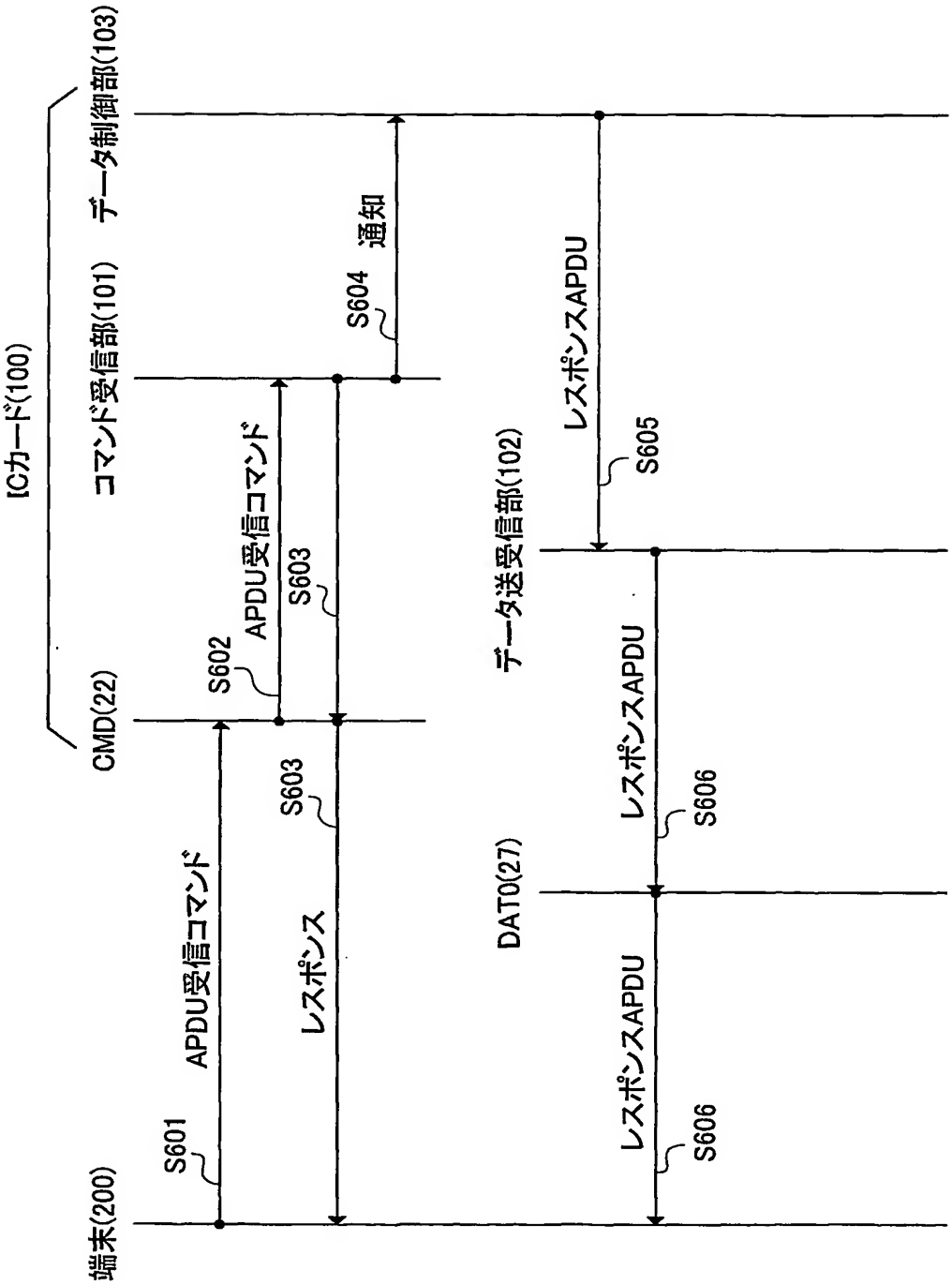

ICカード(100)
端末(200)
CMD(22)
DAT0(27)
コマンド受信部(101)
データ制御部(103)
データ送受信部(102)
S601
APDU受信コマンド
S602
APDU受信コマンド
S603
レスポンス
S603
S604
通知
レスポンスAPDU
S605
レスポンスAPDU
S606
レスポンスAPDU
S606

図8

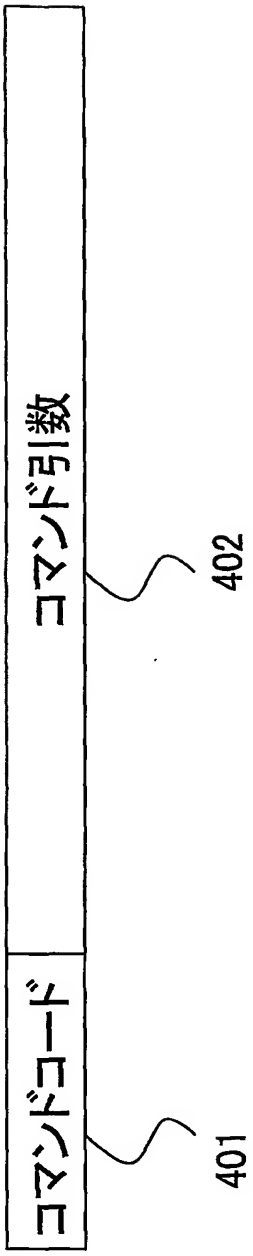


図9

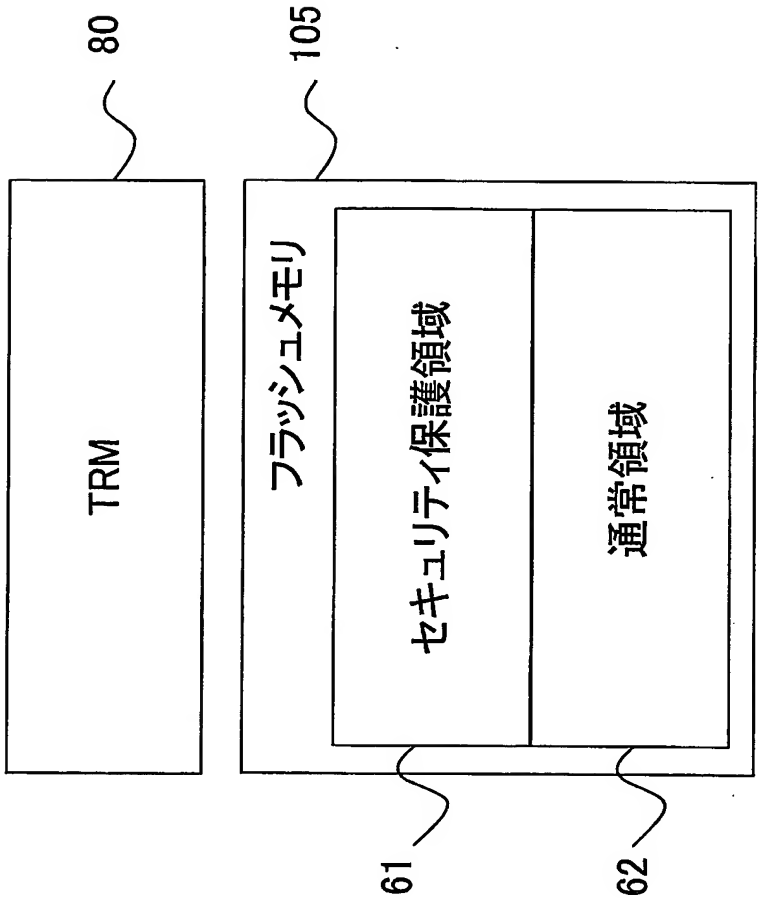


図10

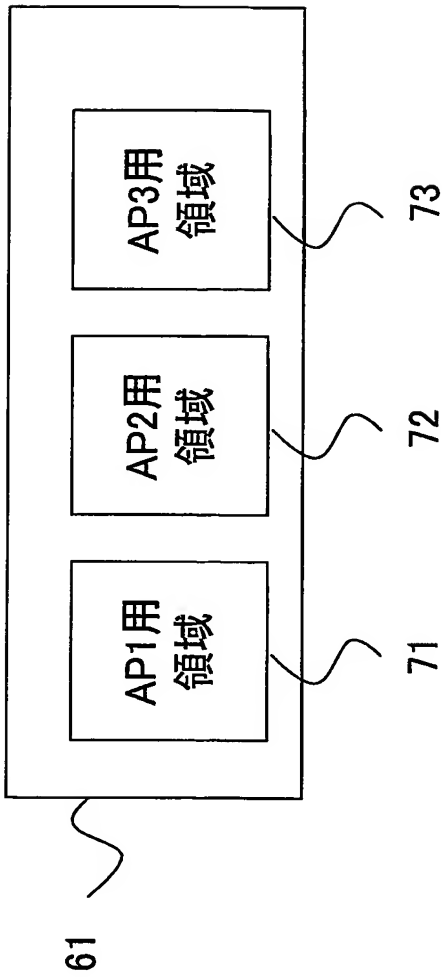


図11

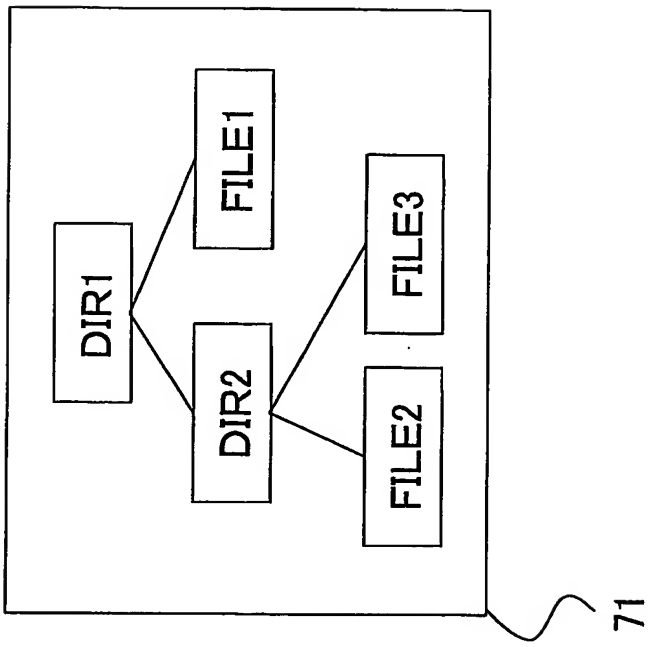


図12

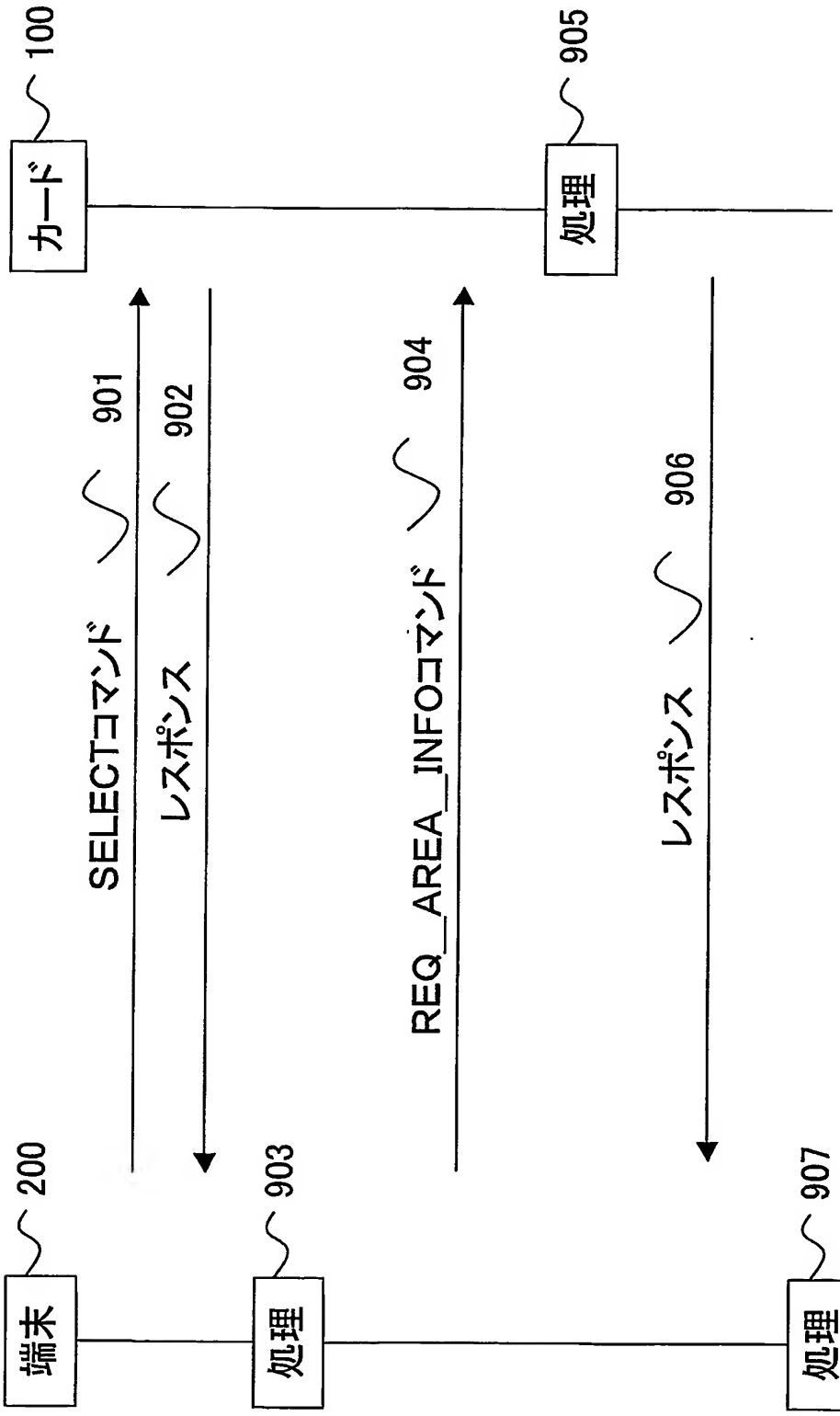

100
カード
905
処理
901
SELECTコマンド
902
レスポンス
904
REQ_AREA_INFOコマンド
906
レスポンス
200
端末
903
処理
907
処理

図13

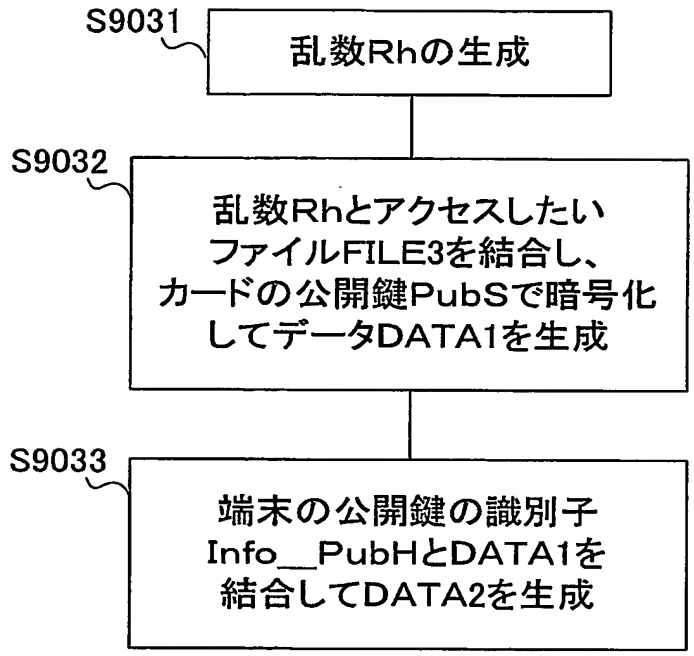

S9031
乱数Rhの生成
S9032
乱数Rhとアクセスしたい
ファイルFILE3を結合し、
カードの公開鍵PubSで暗号化
してデータDATA1を生成
S9033
端末の公開鍵の識別子
Info__PubHとDATA1を
結合してDATA2を生成

図14

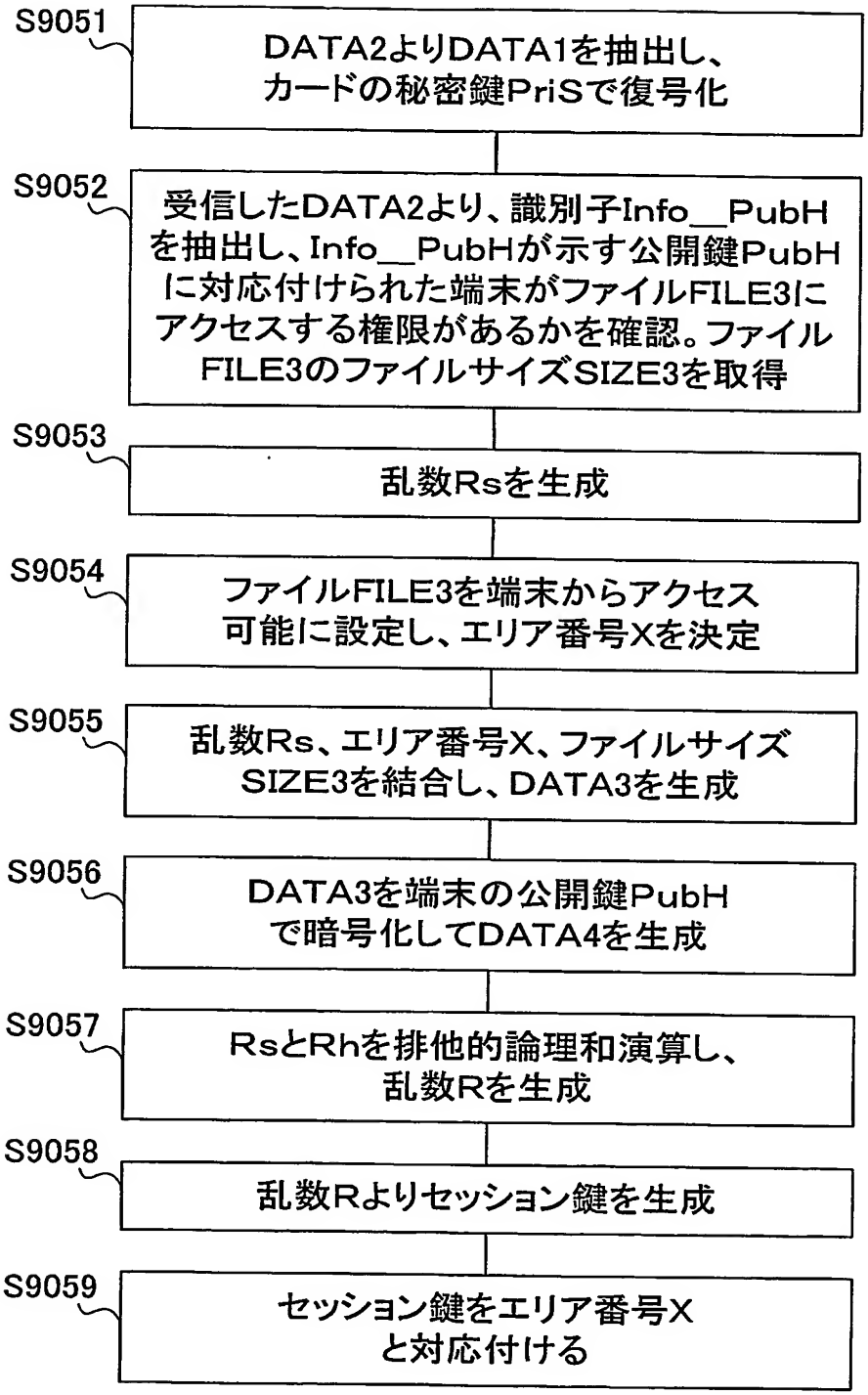

S9051
DATA2よりDATA1を抽出し、
カードの秘密鍵PriSで復号化
S9052
受信したDATA2より、識別子Info__PubH
を抽出し、Info__PubHが示す公開鍵PubH
に対応付けられた端末がファイルFILE3に
アクセスする権限があるかを確認。ファイル
FILE3のファイルサイズSIZE3を取得
S9053
乱数Rsを生成
S9054
ファイルFILE3を端末からアクセス
可能に設定し、エリア番号Xを決定
S9055
乱数Rs、エリア番号X、ファイルサイズ
SIZE3を結合し、DATA3を生成
S9056
DATA3を端末の公開鍵PubH
で暗号化してDATA4を生成
S9057
RsとRhを排他的論理和演算し、
乱数Rを生成
S9058
乱数Rよりセッション鍵を生成
S9059
セッション鍵をエリア番号X
と対応付ける

図15

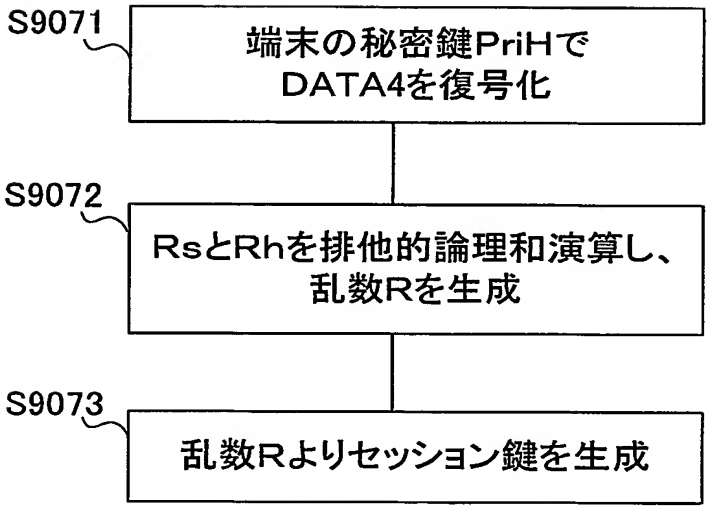

S9071
端末の秘密鍵PriHで
DATA4を復号化
S9072
RsとRhを排他的論理和演算し、
乱数Rを生成
S9073
乱数Rよりセッション鍵を生成

図16

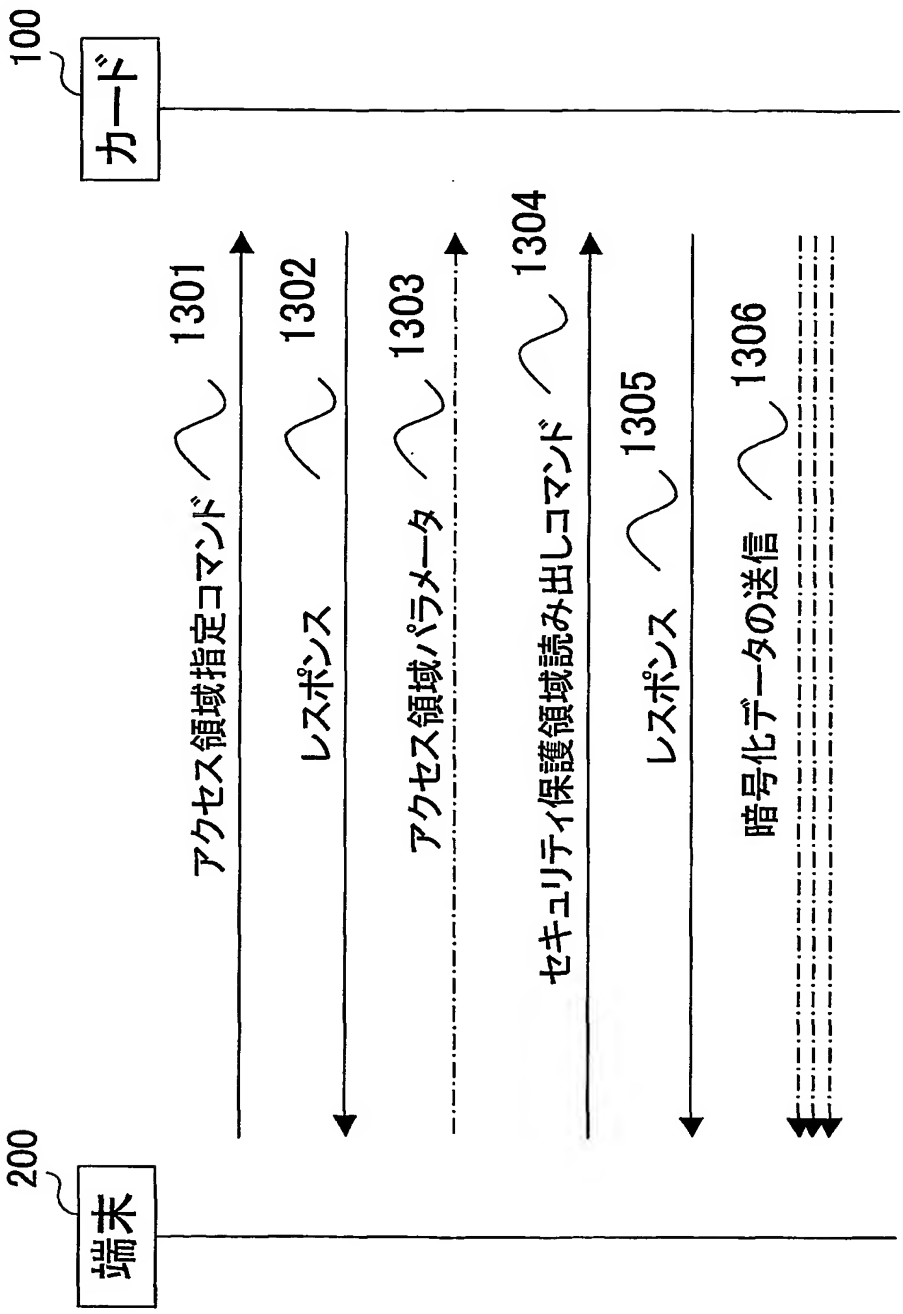

100
カード
200
端末
アクセス領域指定コマンド
1301
レスポンス
1302
アクセス領域パラメータ
1303
セキュリティ保護領域読み出しコマンド
1304
レスポンス
1305
暗号化データの送信
1306

図17

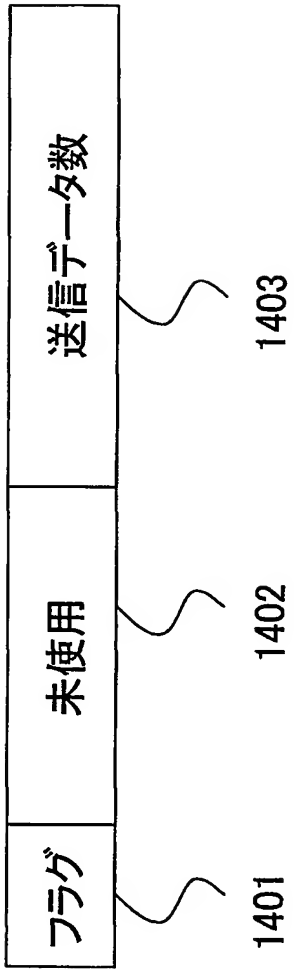


図18

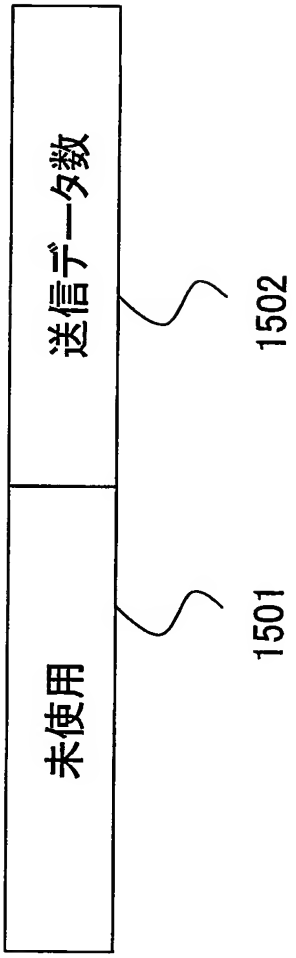


図19

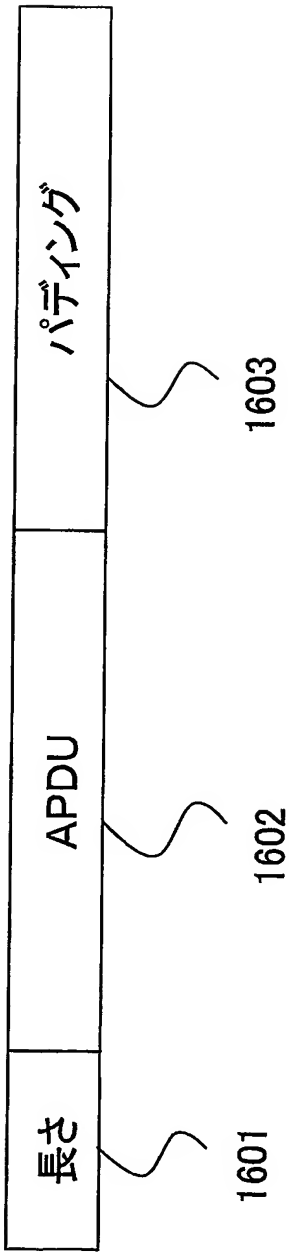


図20

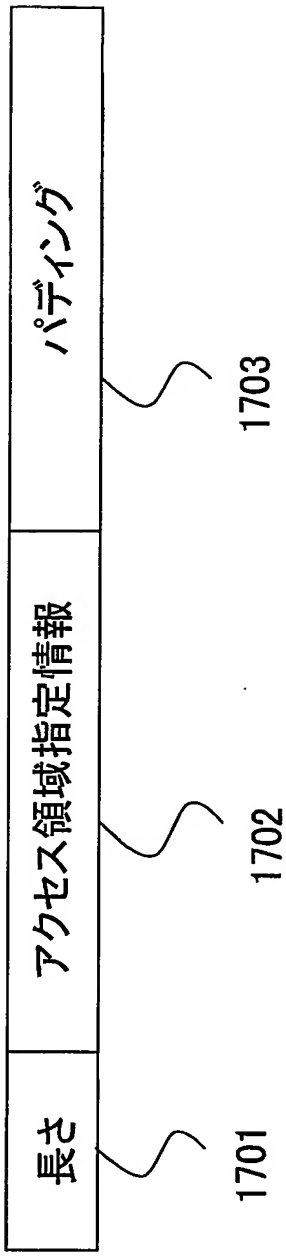


図21

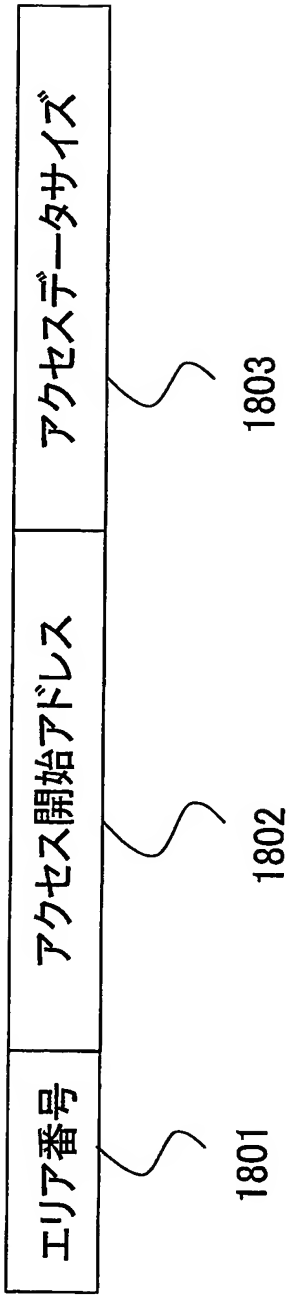


図22

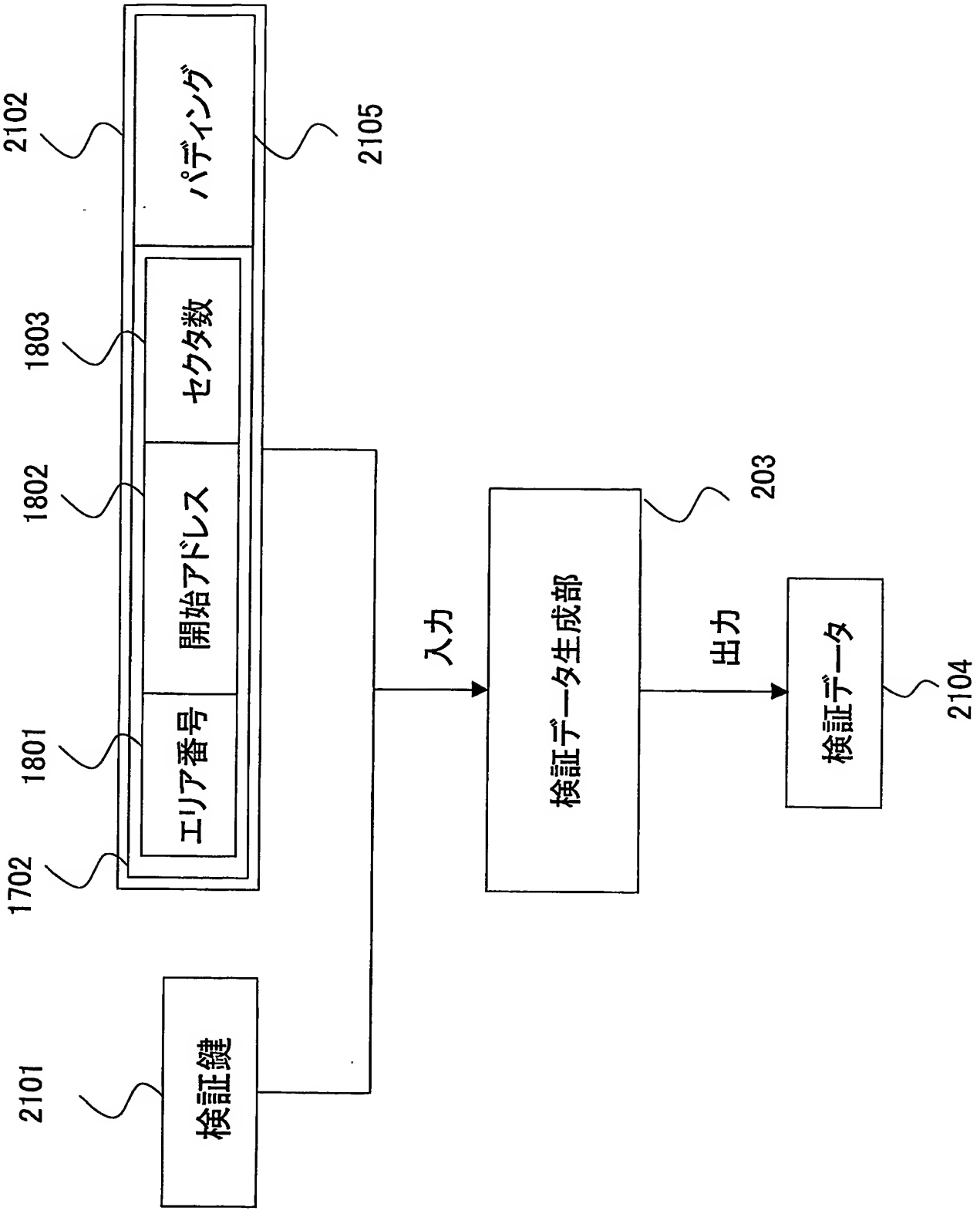

2102
パディング
2105
1803
セクタ数
1802
開始アドレス
1801
エリア番号
1702
2101
検証鍵
入力
検証データ生成部
203
出力
検証データ
2104

図23

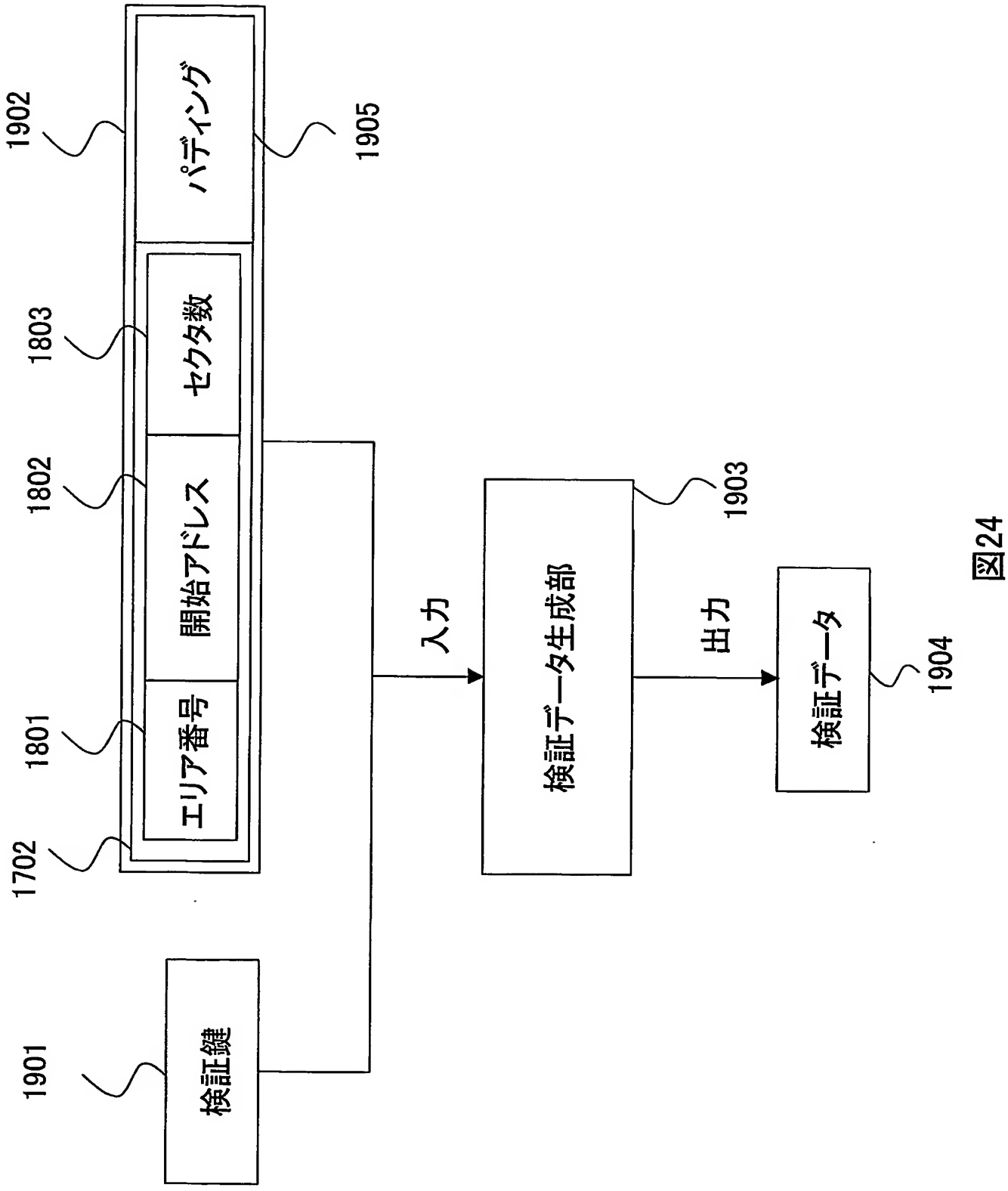

1902
パディング
1905
1803
セクタ数
1802
開始アドレス
1801
エリア番号
1702
1901
検証鍵
入力
検証データ生成部
1903
出力
検証データ
1904

図24

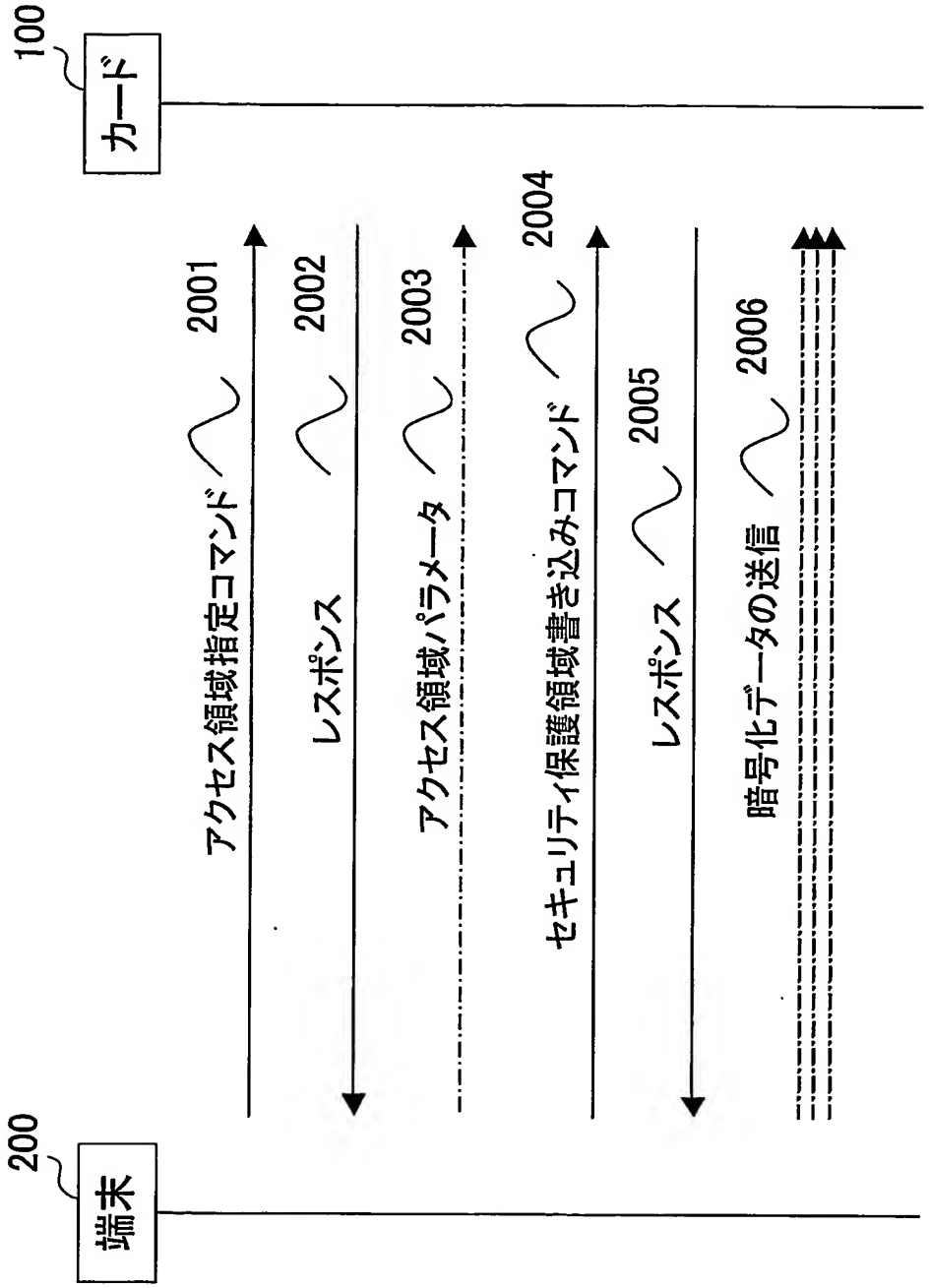

100
カード
200
端末
アクセス領域指定コマンド
2001
レスポンス
2002
アクセス領域パラメータ
2003
セキュリティ保護領域書き込みコマンド
2004
レスポンス
2005
暗号化データの送信
2006

図25

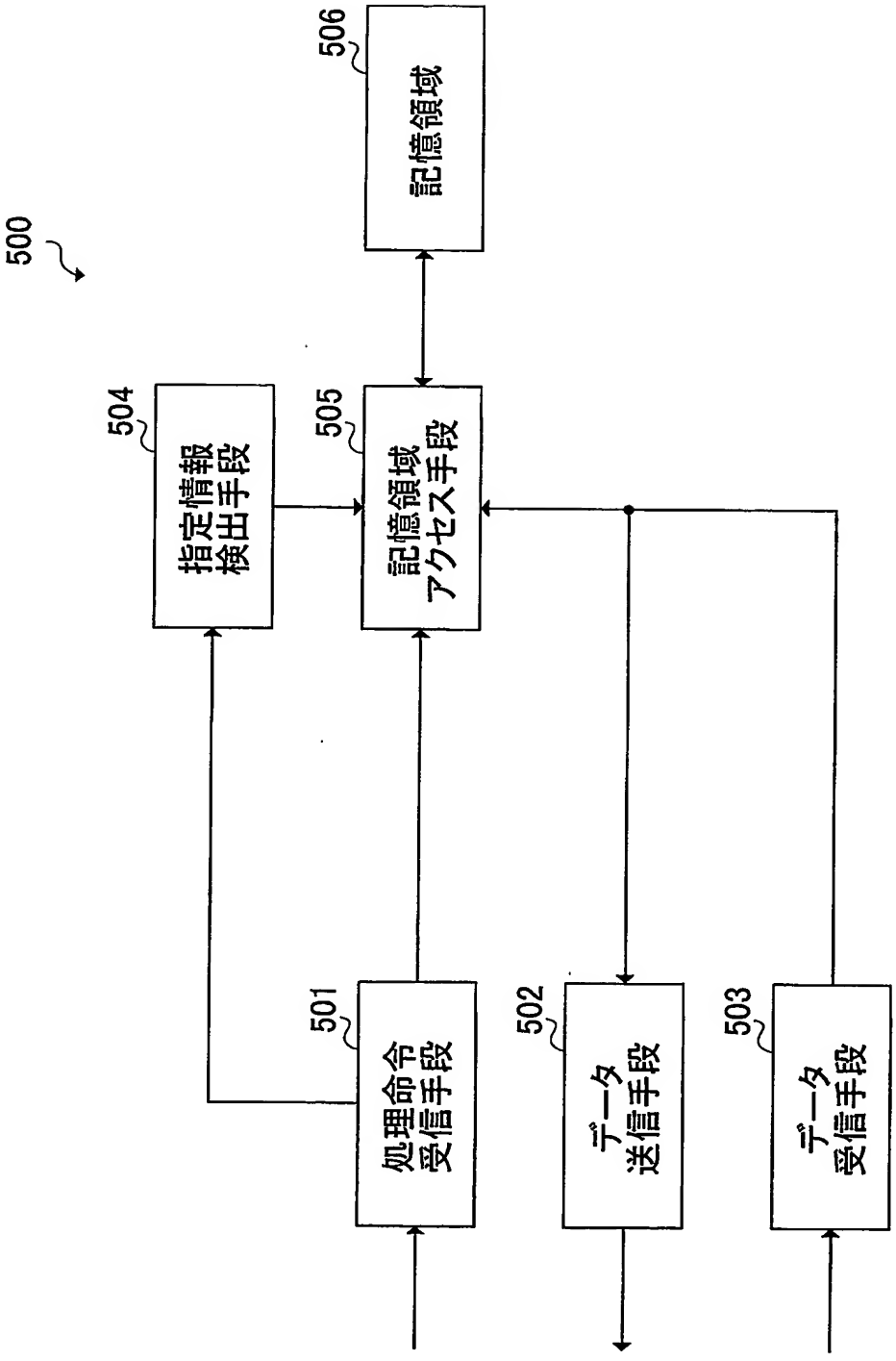

500
506
記憶領域
504
指定情報
検出手段
505
記憶領域
アクセス手段
501
処理命令
受信手段
502
データ
送信手段
503
データ
受信手段

図26

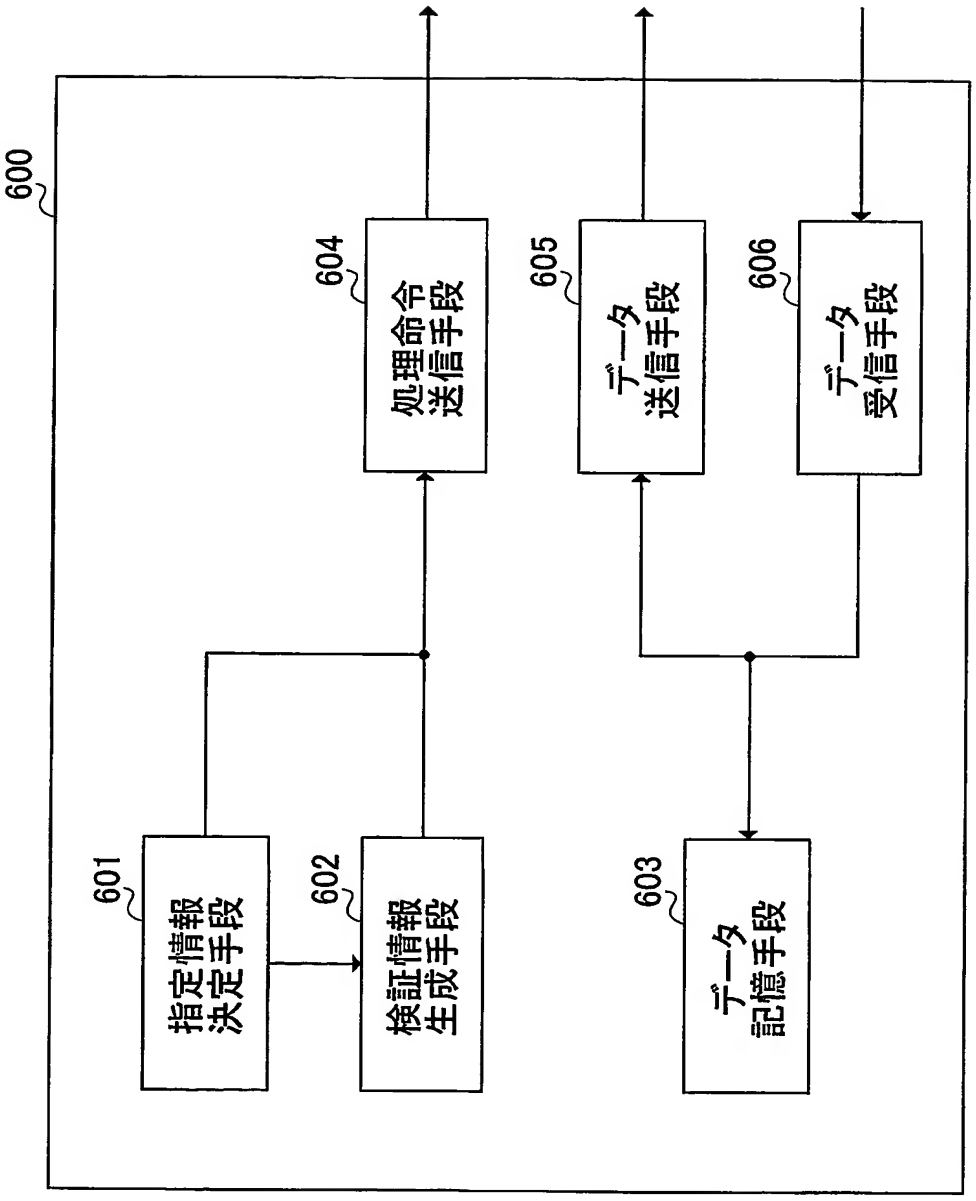

600
601
指定情報
決定手段
602
検証情報
生成手段
603
データ
記憶手段
604
処理命令
送信手段
605
データ
送信手段
606
データ
受信手段

図27

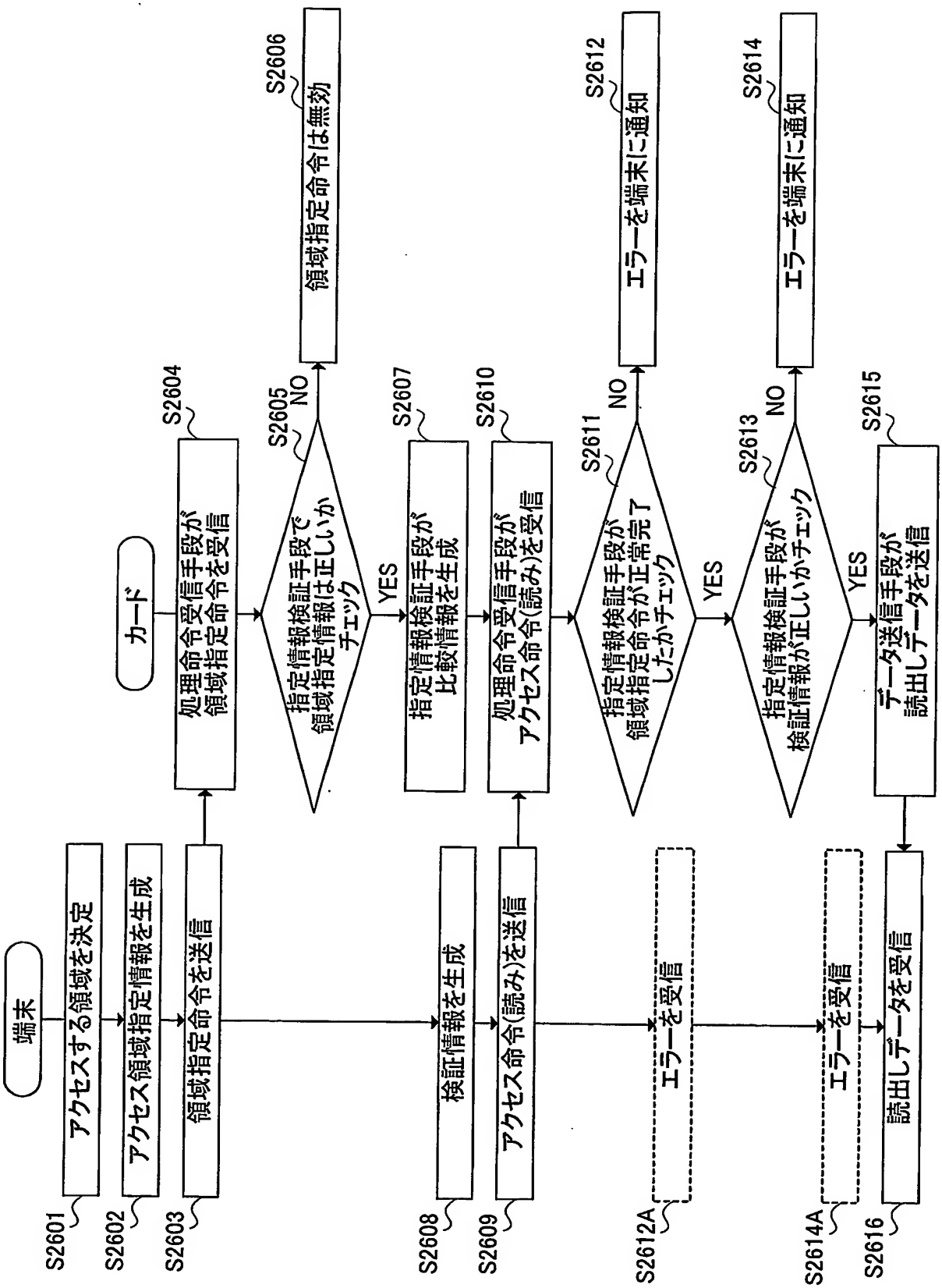

端末
アクセスする領域を決定
アクセス領域指定情報を生成
領域指定命令を送信
S2601
S2602
S2603
カード
処理命令受信手段が
領域指定命令を受信
S2604
指定情報検証手段で
領域指定情報は正しいか
チェック
S2605
NO
YES
領域指定命令は無効
S2606
検証情報を生成
S2608
指定情報検証手段が
比較情報を生成
S2607
アクセス命令(読み)を送信
S2609
処理命令受信手段が
アクセス命令(読み)を受信
S2610
エラーを受信
S2612A
指定情報検証手段が
領域指定命令が正常完了
したかチェック
S2611
NO
YES
エラーを端末に通知
S2612
エラーを受信
S2614A
指定情報検証手段が
検証情報が正しいかチェック
S2613
NO
YES
エラーを端末に通知
S2614
読出しデータを受信
S2616
データ送信手段が
読出しデータを送信
S2615

図28

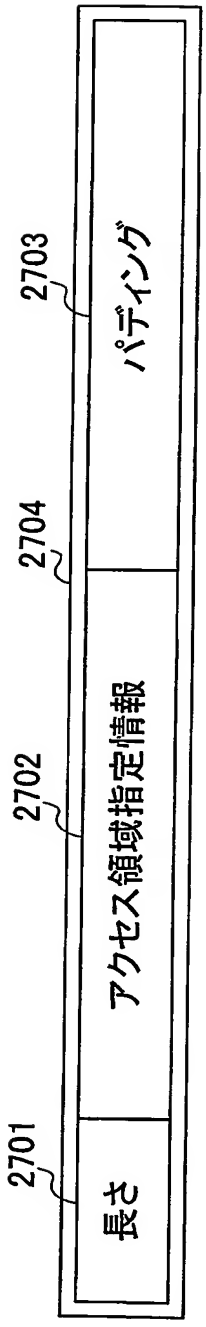


図29

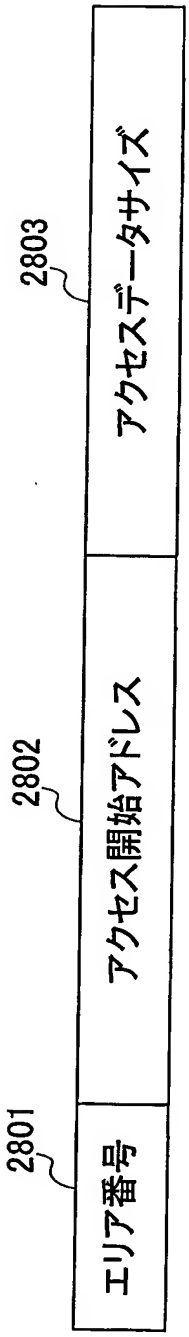


図30

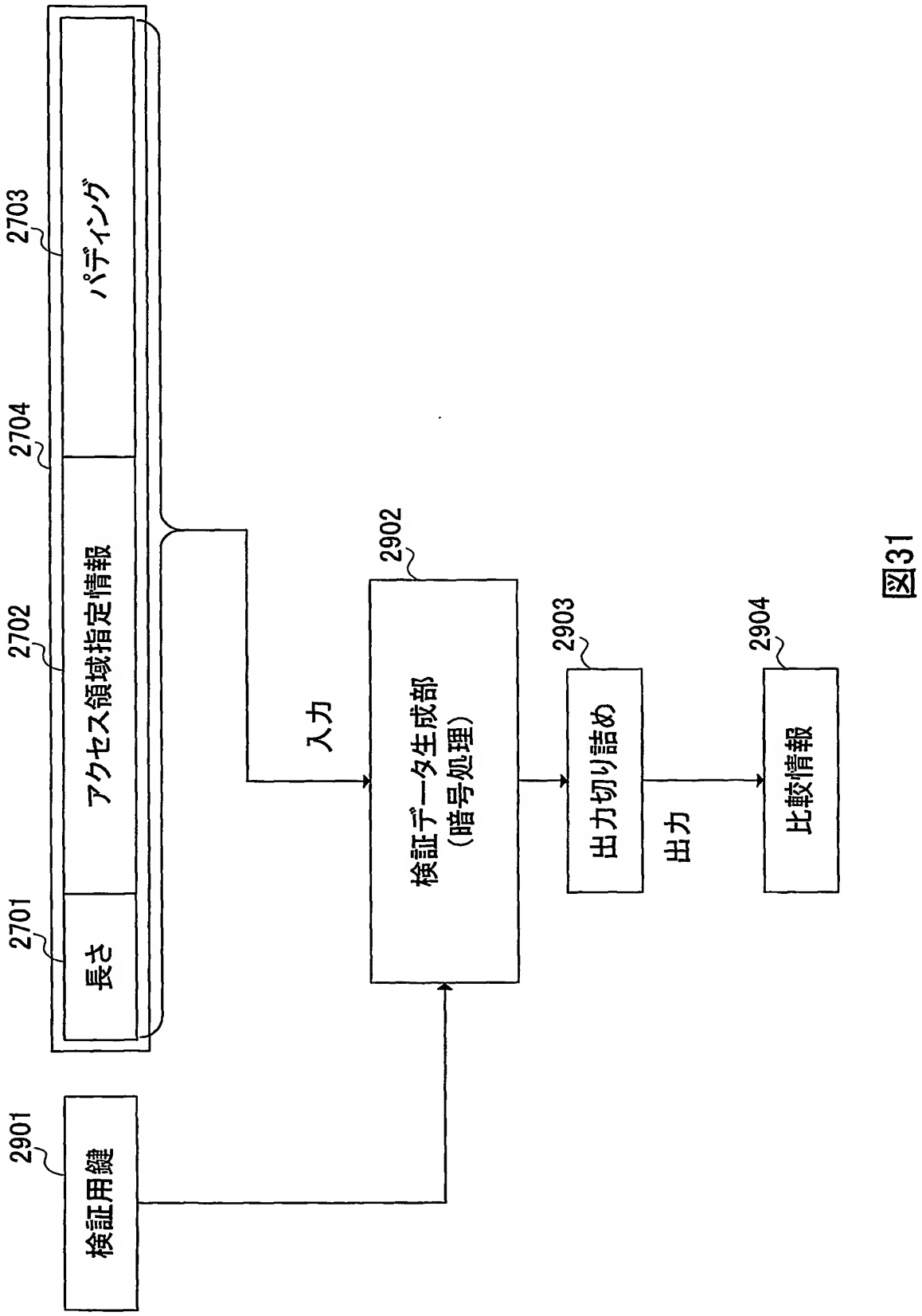

2703
パディング
2704
2702
アクセス領域指定情報
2701
長さ
2901
検証用鍵
入力
2902
検証データ生成部
(暗号処理)
2903
出力切り詰め
出力
2904
比較情報

図31

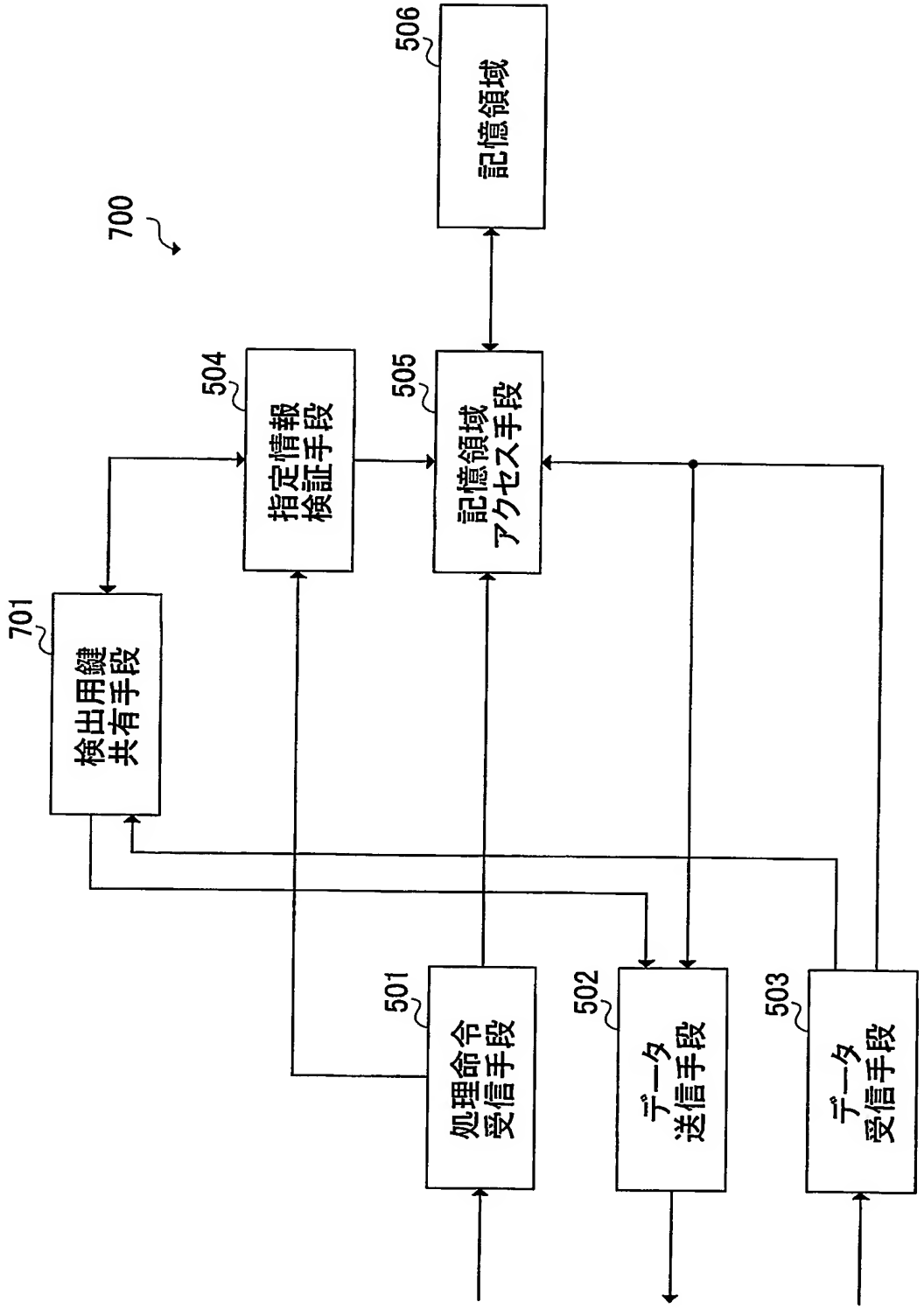

700
506
記憶領域
504
指定情報
検証手段
505
記憶領域
アクセス手段
701
検出用鍵
共有手段
501
処理命令
受信手段
502
データ
送信手段
503
データ
受信手段

図32

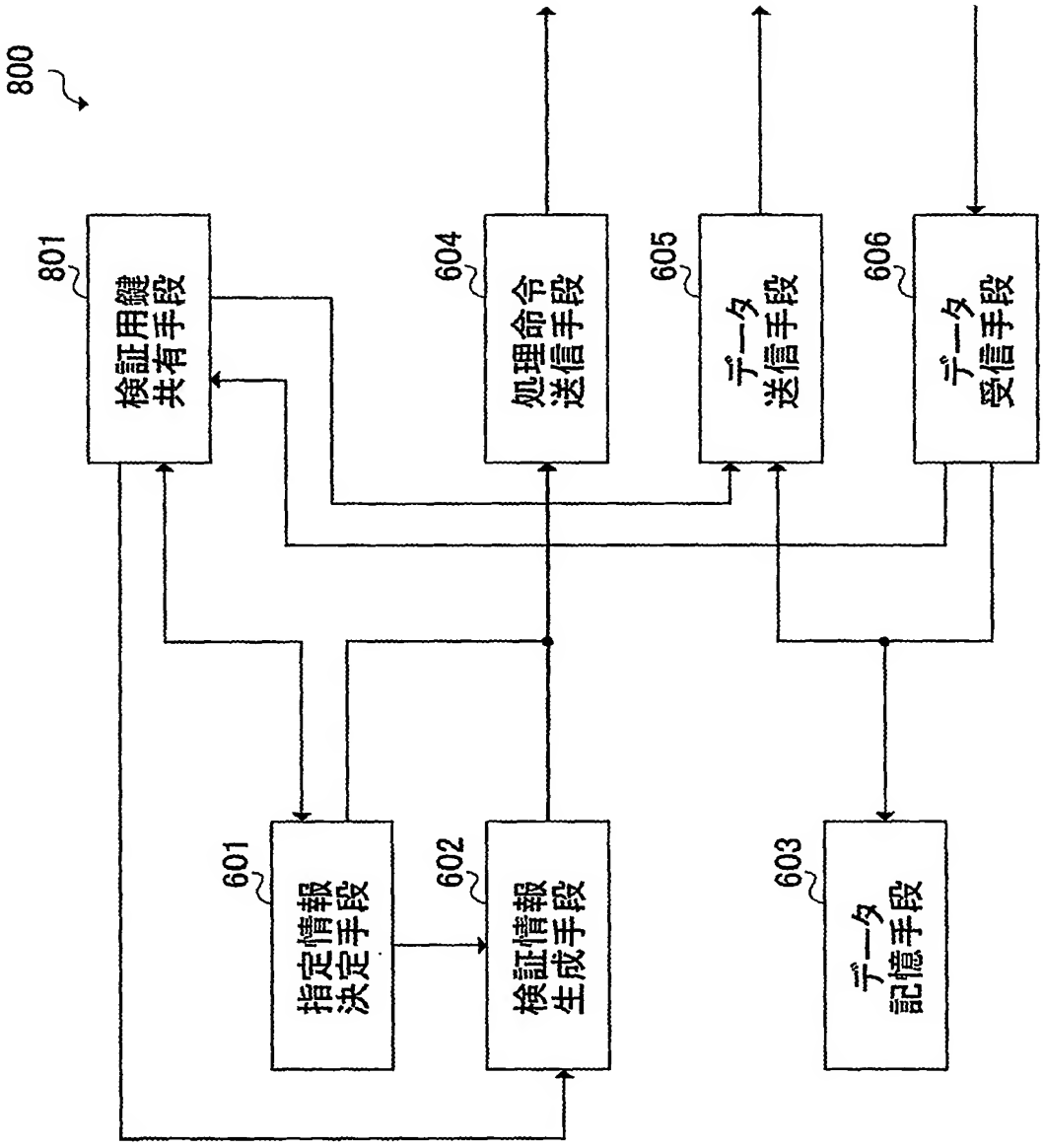

800
801
検証用鍵
共有手段
604
処理命令
送信手段
605
データ
送信手段
606
データ
受信手段
601
指定情報
決定手段
602
検証情報
生成手段
603
データ
記憶手段

図33

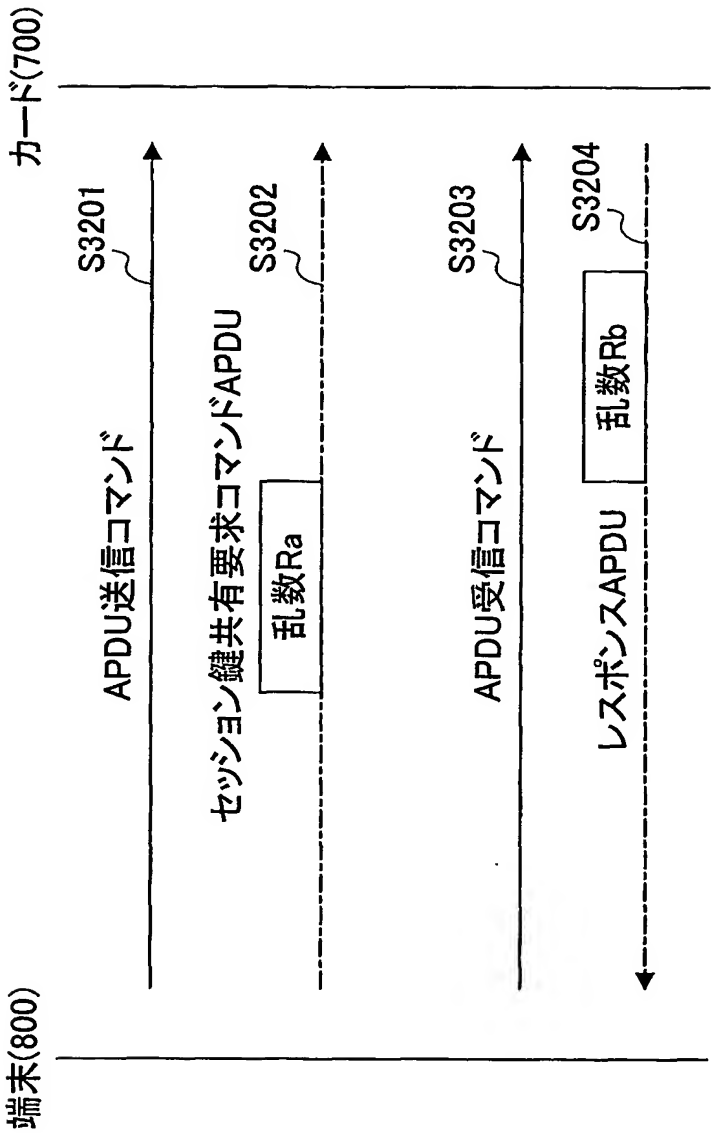

カード(700)
端末(800)
S3201
APDU送信コマンド
S3202
セッション鍵共有要求コマンドAPDU
乱数Ra
S3203
APDU受信コマンド
S3204
レスポンスAPDU
乱数Rb

図34

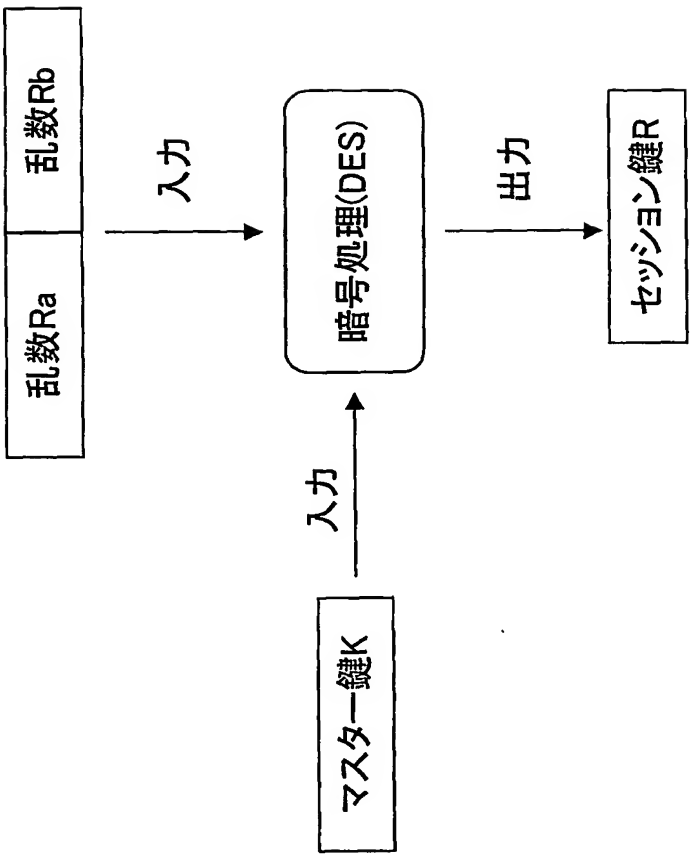


図35

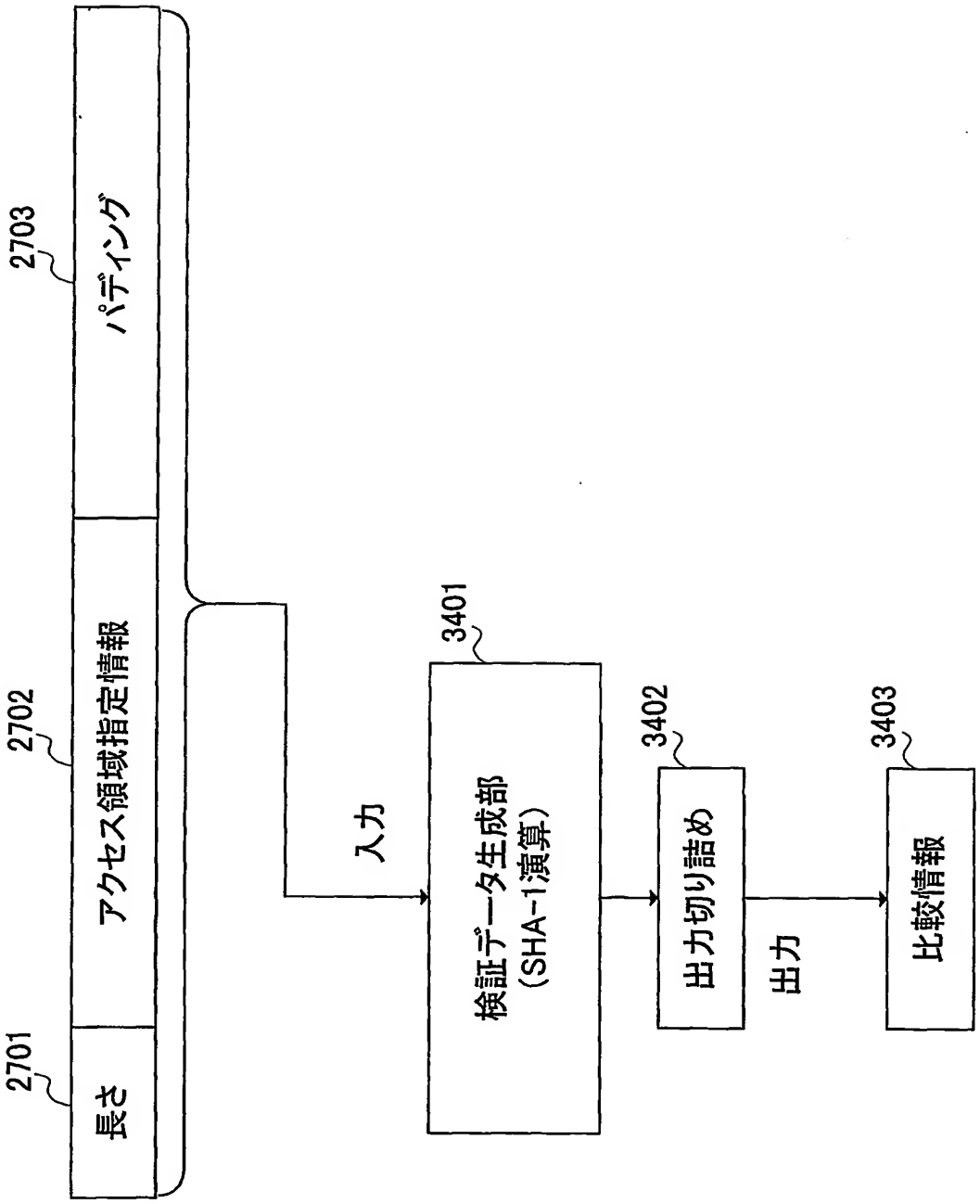

2703
パディング
2702
アクセス領域指定情報
2701
長さ
入力
3401
検証データ生成部
(SHA-1演算)
3402
出力切り詰め
出力
3403
比較情報

図36

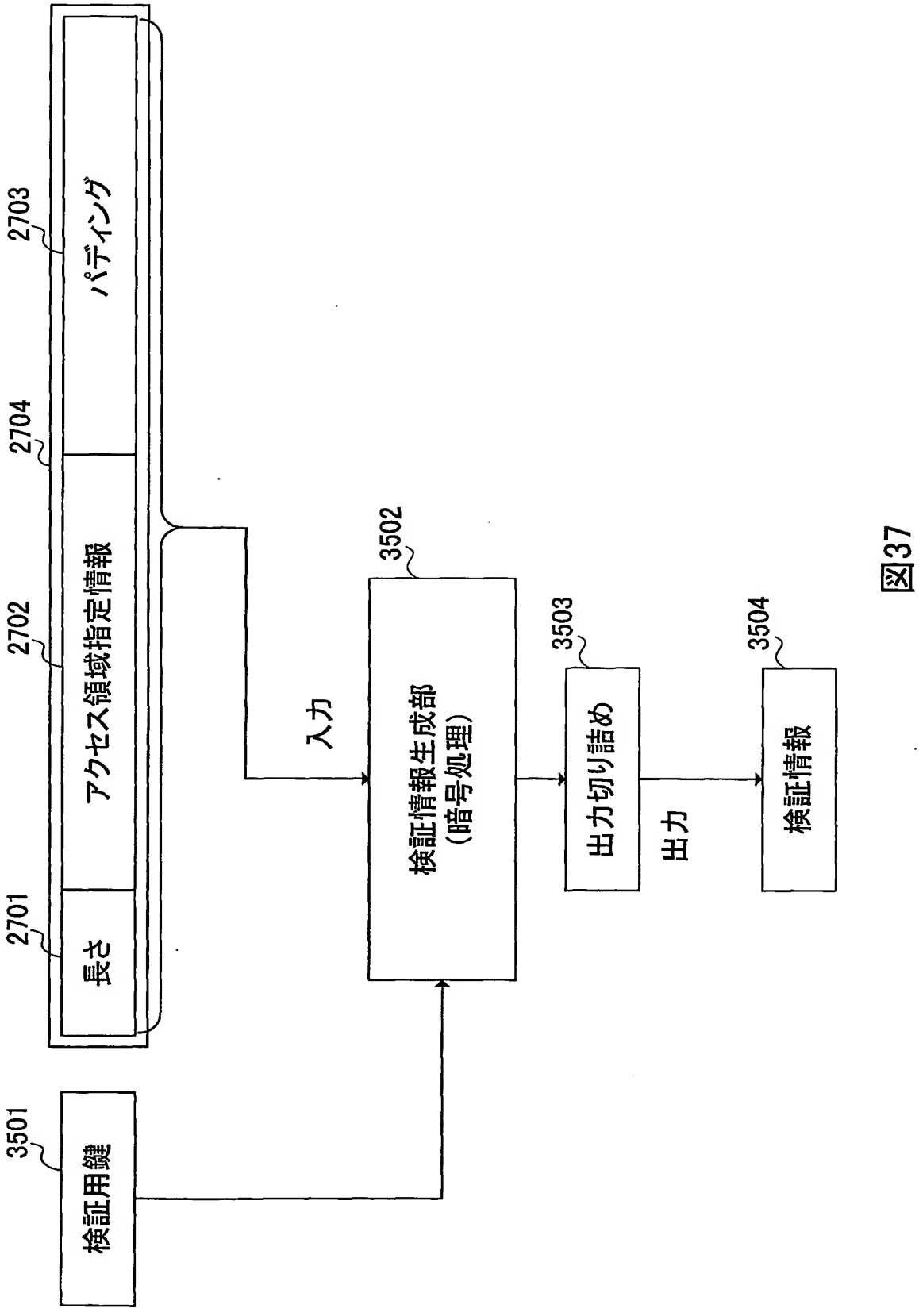

2703
パディング
2704
2702
アクセス領域指定情報
2701
長さ
3501
検証用鍵
入力
3502
検証情報生成部
(暗号処理)
3503
出力切り詰め
出力
3504
検証情報

図37

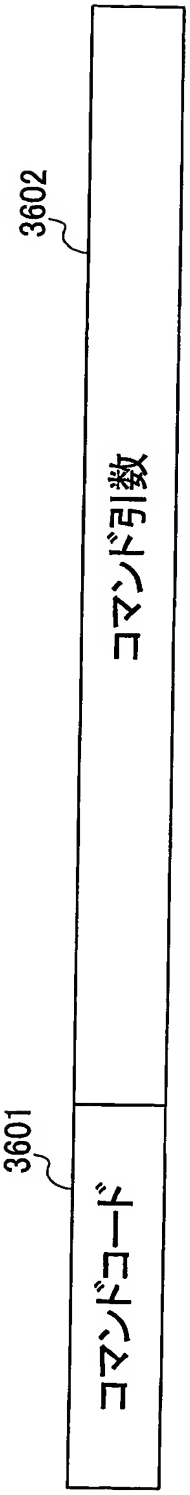


図38

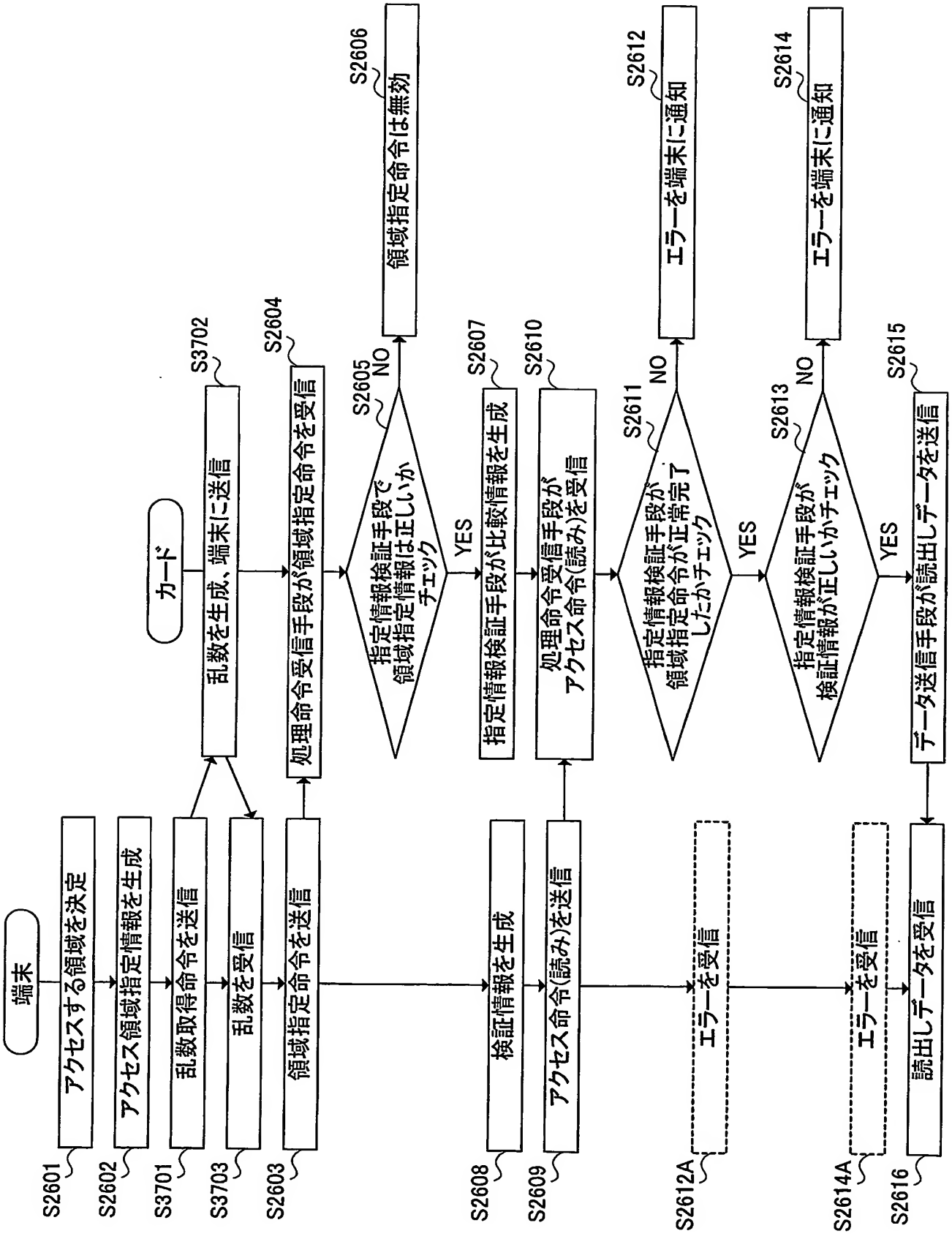

端末
カード
S2601 アクセスする領域を決定
S2602 アクセス領域指定情報を生成
S3701 乱数取得命令を送信
S3703 乱数を受信
S2603 領域指定命令を送信
S3702 乱数を生成、端末に送信
S2604 処理命令受信手段が領域指定命令を受信
S2605 指定情報検証手段で領域指定情報は正しいかチェック
NO
S2606 領域指定命令は無効
YES
S2607 指定情報検証手段が比較情報を生成
S2608 検証情報を生成
S2609 アクセス命令(読み)を送信
S2610 処理命令受信手段がアクセス命令(読み)を受信
S2611 指定情報検証手段が領域指定命令が正常完了したかチェック
NO
S2612 エラーを端末に通知
YES
S2612A エラーを受信
S2613 指定情報検証手段が検証情報が正しいかチェック
NO
S2614 エラーを端末に通知
YES
S2614A エラーを受信
S2615 データ送信手段が読出しデータを送信
S2616 読出しデータを受信

図39

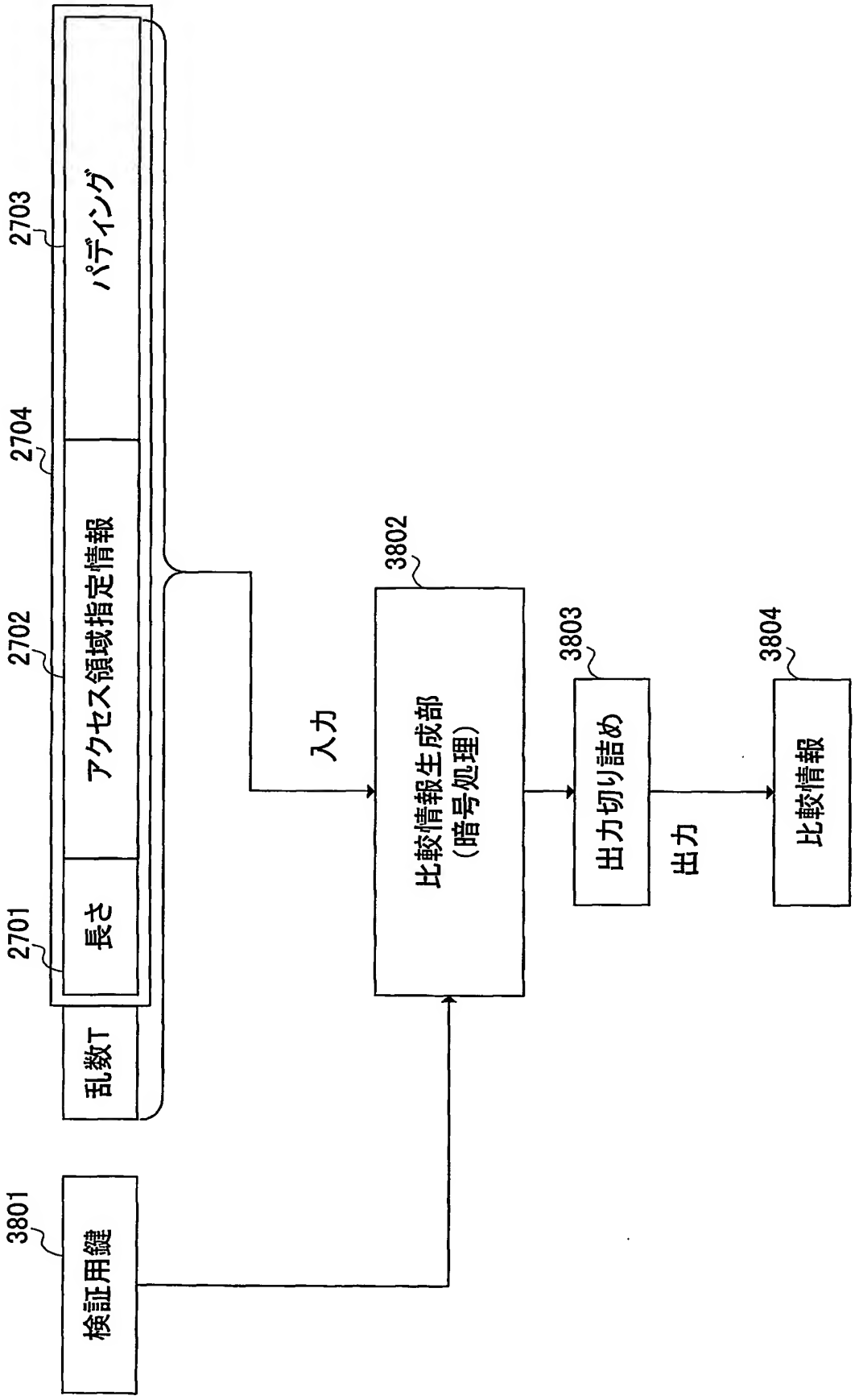

2703
パディング
2704
アクセス領域指定情報
2702
2701
長さ
乱数T
入力
3802
比較情報生成部
(暗号処理)
3803
出力切り詰め
出力
3804
比較情報
3801
検証用鍵

図40

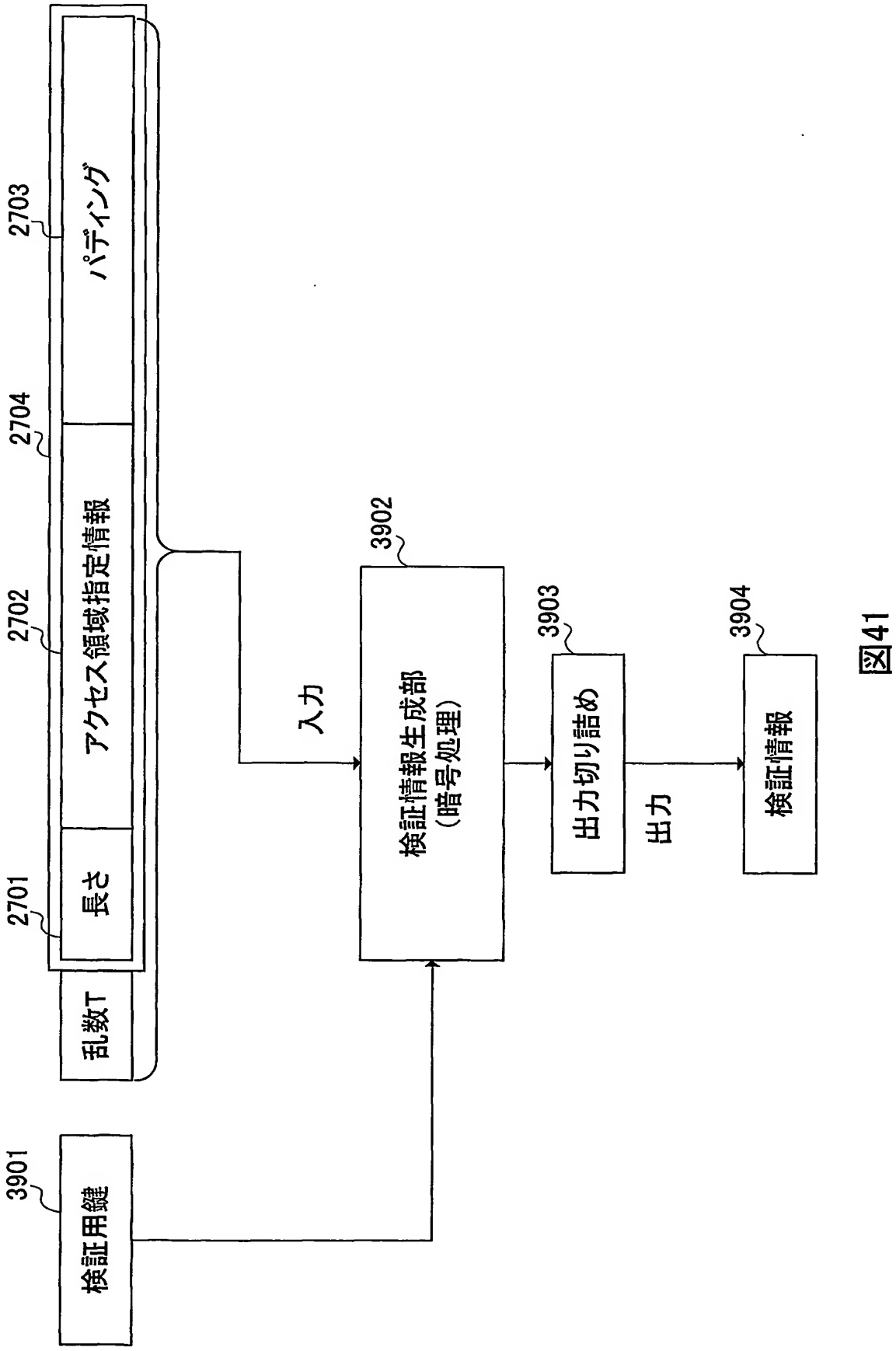

2703
パディング
2704
アクセス領域指定情報
2702
2701
長さ
乱数T
入力
3902
検証情報生成部
(暗号処理)
3903
出力切り詰め
出力
3904
検証情報
3901
検証用鍵

図41

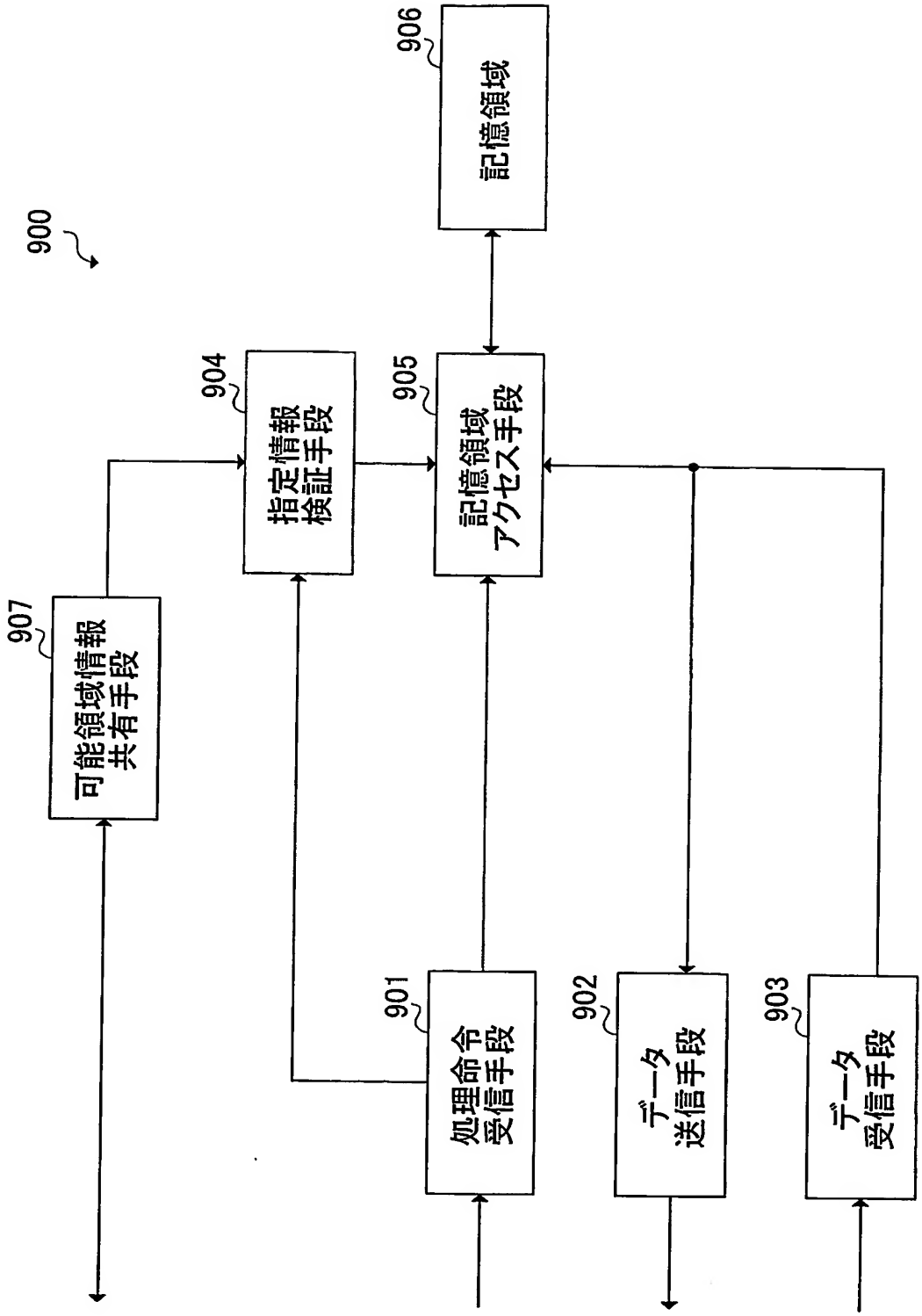

900
906
記憶領域
904
指定情報
検証手段
905
記憶領域
アクセス手段
907
可能領域情報
共有手段
901
処理命令
受信手段
902
データ
送信手段
903
データ
受信手段

図42

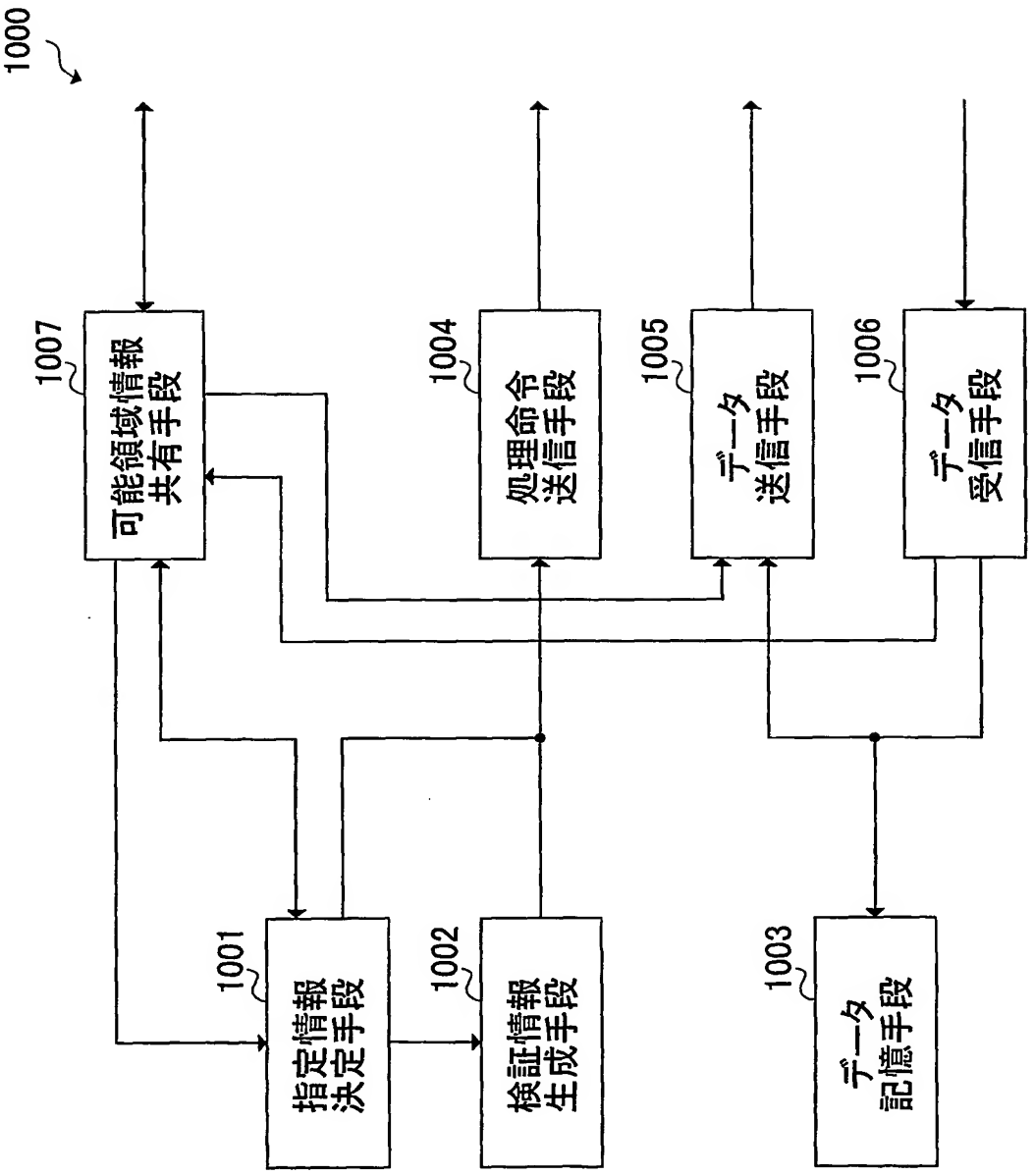

1000
1007
可能領域情報
共有手段
1004
処理命令
送信手段
1005
データ
送信手段
1006
データ
受信手段
1001
指定情報
決定手段
1002
検証情報
生成手段
1003
データ
記憶手段

図43

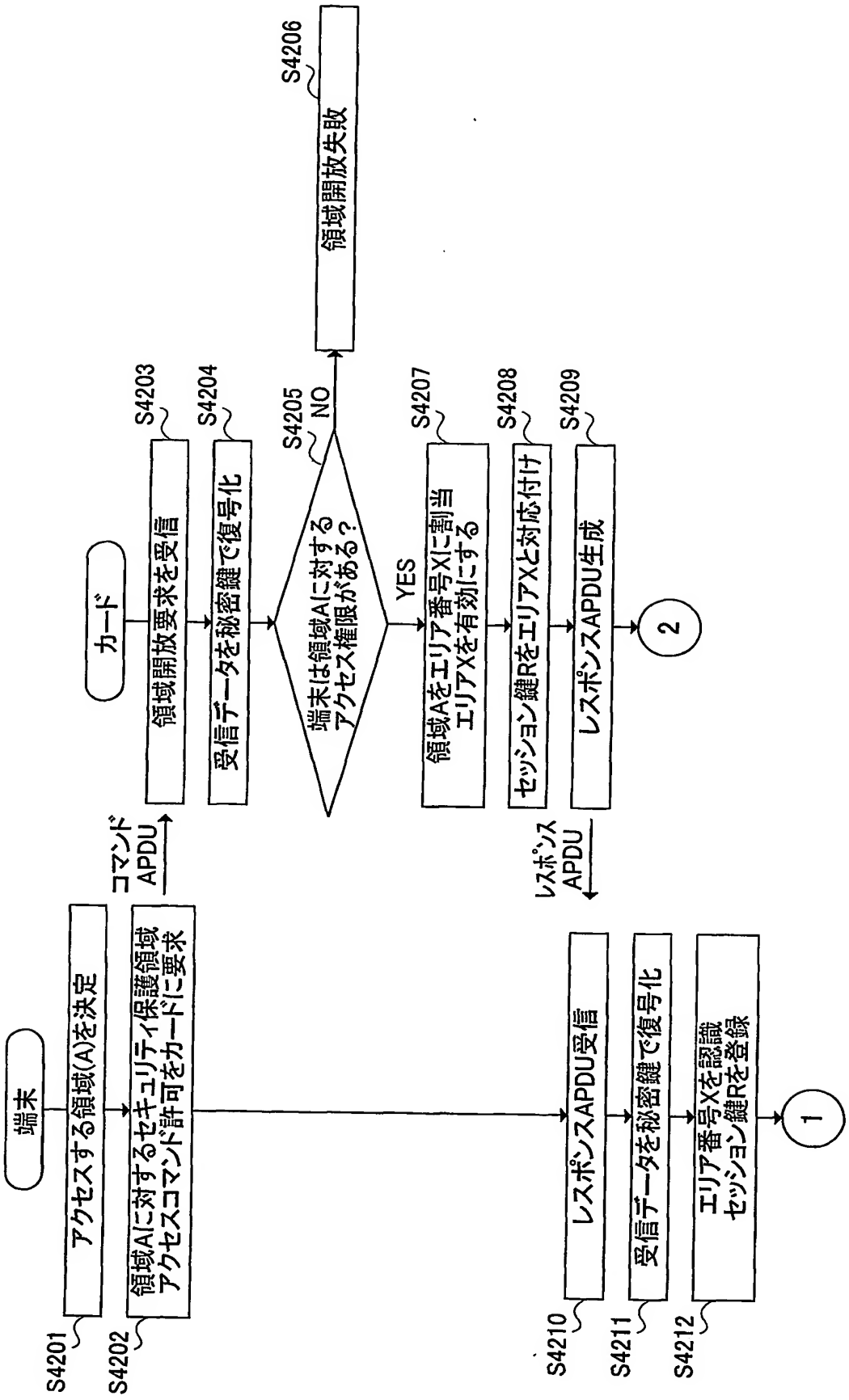

端末
アクセスする領域(A)を決定
S4201
領域Aに対するセキュリティ保護領域
アクセスコマンド許可をカードに要求
S4202
コマンド
APDU
カード
領域開放要求を受信
S4203
受信データを秘密鍵で復号化
S4204
端末は領域Aに対する
アクセス権限がある？
S4205
NO
領域開放失敗
S4206
YES
領域Aをエリア番号Xに割当
エリアXを有効にする
S4207
セッション鍵Rをエリアxと対応付け
S4208
レスポンスAPDU生成
S4209
2
レスポンス
APDU
レスポンスAPDU受信
S4210
受信データを秘密鍵で復号化
S4211
エリア番号Xを認識
セッション鍵Rを登録
S4212
1

図44

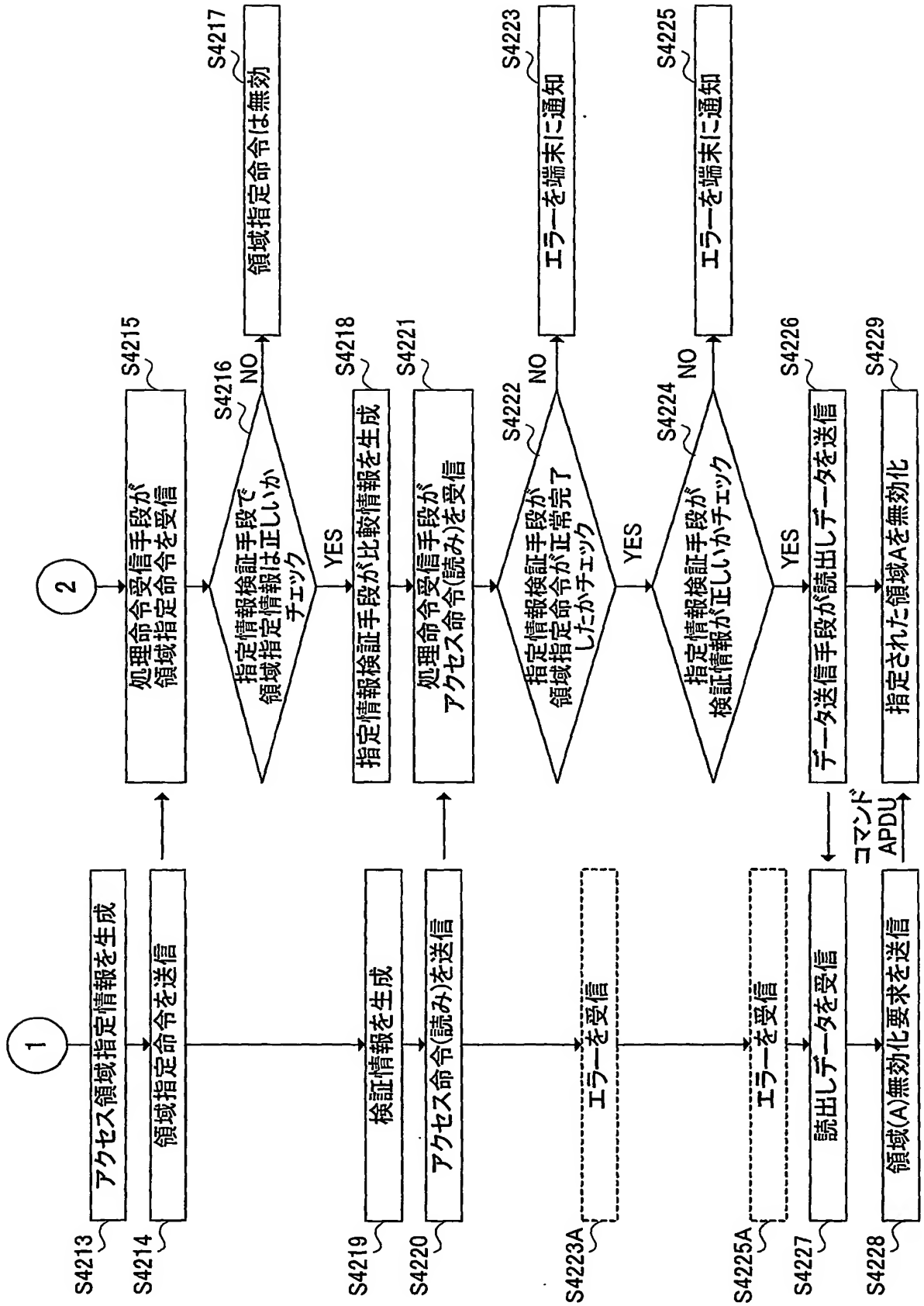

1
アクセス領域指定情報を生成
S4213
領域指定命令を送信
S4214
2
処理命令受信手段が領域指定命令を受信
S4215
指定情報検証手段で領域指定情報は正しいかチェック
S4216
NO
領域指定命令は無効
S4217
YES
指定情報検証手段が比較情報を生成
S4218
検証情報を生成
S4219
処理命令受信手段がアクセス命令(読み)を受信
S4221
アクセス命令(読み)を送信
S4220
指定情報検証手段が領域指定命令が正常完了したかチェック
S4222
NO
エラーを端末に通知
S4223
エラーを受信
S4223A
YES
指定情報検証手段が検証情報が正しいかチェック
S4224
NO
エラーを端末に通知
S4225
エラーを受信
S4225A
YES
データ送信手段が読出しデータを送信
S4226
読出しデータを受信
S4227
コマンドAPDU
領域(A)無効化要求を送信
S4228
指定された領域Aを無効化
S4229

図45

4400

エリア番号X	領域識別子a	検証用鍵R
エリア番号2	領域識別子b	検証用鍵
エリア番号3	領域識別子c	検証用鍵
・・・	・・・	・・・

図46

4500

エリア番号X	FILE3	セッション鍵Km
エリア番号2	ファイル識別子2	セッション鍵
エリア番号3	ファイル識別子4	セッション鍵
・・・	・・・	・・・

図47

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/010432

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/14, G06K17/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/14, G06K17/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Toroku Jitsuyo Shinan Koho 1994-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 11-306088 A (Toppan Printing Co., Ltd.), 05 November, 1999 (05.11.99), Full text; all drawings (Family: none)	1-19
Y	JP 1-147686 A (Toshiba Corp.), 09 June, 1989 (09.06.89), Full text; all drawings (Family: none)	1-19
Y	JP 2001-118034 A (Toshiba Corp.), 27 April, 2001 (27.04.01), Full text; all drawings (Family: none)	3-4,6,8,11, 15,18-19

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 October, 2004 (20.10.04)	09 November, 2004 (09.11.04)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/010432

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 7-78126 A (Kyodo Printing Co., Ltd.), 20 March, 1995 (20.03.95), Par. No. [0018]; Fig. 4 (Family: none)	7-8,19

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／０１０４３２

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ．⁷　Ｇ０６Ｆ　１２／１４，Ｇ０６Ｋ　１７／００

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ．⁷　Ｇ０６Ｆ　１２／１４，Ｇ０６Ｋ　１７／００

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　　１９２２－１９９６年
日本国公開実用新案公報　１９７１－２００４年
日本国実用新案登録公報　１９９６－２００４年
日本国登録実用新案公報　１９９４－２００４年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ　１１－３０６０８８　Ａ（凸版印刷株式会社） １９９９．１１．０５，全文，全図（ファミリーなし）	１－１９
Ｙ	ＪＰ　１－１４７６８６　Ａ（株式会社東芝） １９８９．０６．０９，全文，全図（ファミリーなし）	１－１９
Ｙ	ＪＰ　２００１－１１８０３４　Ａ（株式会社東芝） ２００１．０４．２７，全文，全図（ファミリーなし）	３－４，６，８，１１，１５，１８－１９

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
20.10.2004	09.11.2004

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	桜井 茂行	５Ｎ	２９４５
	電話番号　０３－３５８１－１１０１　内線　３５８５		

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００４年１月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／０１０４３２

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ ７－７８１２６ Ａ（共同印刷株式会社） １９９５．０３．２０，【００１８】段落，第４図（ファミリーなし）	７－８，１９

様式ＰＣＴ／ＩＳＡ／２１０（第２ページの続き）（２００４年１月）